Estudo Técnico Preliminar 77/2024

1. Informações Básicas

Número do processo: 80000.000362/2024-15

2. Descrição da necessidade

Nos últimos anos, a compreensão do valor dos dados como ativos intangíveis se intensificou, impulsionada pelo avanço tecnológico que transformou os processos de produção e armazenamento de informações. Para instituições como o Ministério das Cidades (MCID), que operam em ambientes cada vez mais conectados, a segurança da informação se torna uma prioridade. A utilização da Internet e de redes parceiras, embora traga oportunidades significativas de conectividade e lucro, também expõe as organizações a riscos consideráveis, incluindo infestações, adulteração, roubo de dados e ataques maliciosos.

O fluxo crescente de informações e a necessidade de disponibilização online de aplicações têm apresentado desafios significativos à segurança da informação e das comunicações no MCID. Com a crescente dependência de sistemas e serviços de informação, as ameaças cibernéticas se tornaram mais frequentes e sofisticadas, resultando em falhas de segurança que podem gerar prejuízos financeiros significativos, além de danos à reputação do Ministério.

O Gabinete de Segurança Institucional da Presidência da República (GSI/PR) responsável por coordenar as atividades de segurança da informação e das comunicações no governo federal, por meio da PORTARIA GSI/PR Nº 120, DE 21 DE DEZEMBRO DE 2022,(https://www.in.gov.br/en/web/dou/-/portaria-gsi/pr-n-120-de-21-de-dezembro-de-2022-452767918) deixa claro as orientações para proteção das entidades públicas do executivo federal, ao qual destacamos o item 2 e seu subitem 2.1:

“2. PREVENÇÃO

A prevenção é um processo constante de ações proativas com o objetivo de reduzir a probabilidade de ataques cibernéticos bem-sucedidos. Entre essas ações, enfatizam-se as de definição e de implementação de controles de segurança, de gerência mento de vulnerabilidades, de conscientização e de capacitação.

As ações preventivas de segurança cibernética deverão contemplar aquelas previstas na política de segurança da informação do integrante da Regic.

2.1. Definição e implementação de controles de segurança preventivos:

Os controles de segurança preventivos constituem-se em tecnológicos, organizacionais e físicos.

Os controles tecnológicos são aqueles utilizados para reduzir vulnerabilidades no hardware e no software. Entre os principais de controles tecnológicos estão:

- *dispositivos endpoint do usuário;*
- *restrição de acesso à informação;*
- *autenticação segura;*
- *proteção contra malware;*
- *backup das informações;*
- *atividades de monitora mento (log);*
- *segurança de redes;*
- *uso de criptografia; e*

- *gestão de mudanças.*

Por sua vez, os controles organizacionais são utilizados para assegurar a adequação contínua e efetiva da gestão de segurança da informação. Entre os principais controles organizacionais estão:

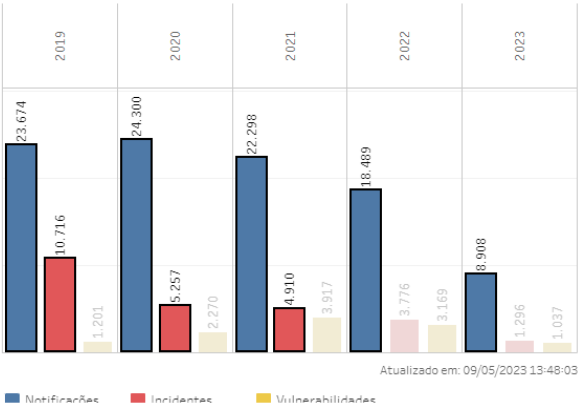
- *política de Segurança da Informação;*
- *definição de papéis e responsabilidades pela segurança da informação;*
- *segregação de funções;*
- *mapeamento de ativos de informação;*
- *controle de acesso;*
- *classificação e rotulagem de informações; e*
- *norma de segurança da informação para uso de serviços em nuvem.*

Por fim, os controles físicos têm por finalidade prevenir ou evitar o acesso não autorizado à área ou material sensível, bem como danos e interferências às áreas que contenham informações críticas ou sensíveis. Entre os principais controles físicos estão:

- *definição dos perímetros de segurança física;*
- *monitoramento de segurança física;*
- *proteção contra ameaças físicas e ambientais;*
- *localização e proteção de equipamentos;*
- *segurança de ativos fora das instalações da organização; e*
- *manutenção de ativos."*

Ainda nesta linha o Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo, entidade que está enquadrada na categoria "CSIRT de responsabilidade nacional de coordenação" publica regularmente relatórios sobre a quantidade de incidentes descobertos. Os dados podem ser acessados em https://www.gov.br/ctir/pt-br/assuntos/ctir-gov-em-numeros/visao-geral.

Abaixo, apresentamos as estatísticas das Notificações Reportadas e Incidentes/Vulnerabilidades Confirmados pelo CTIR Gov ao longo do tempo:

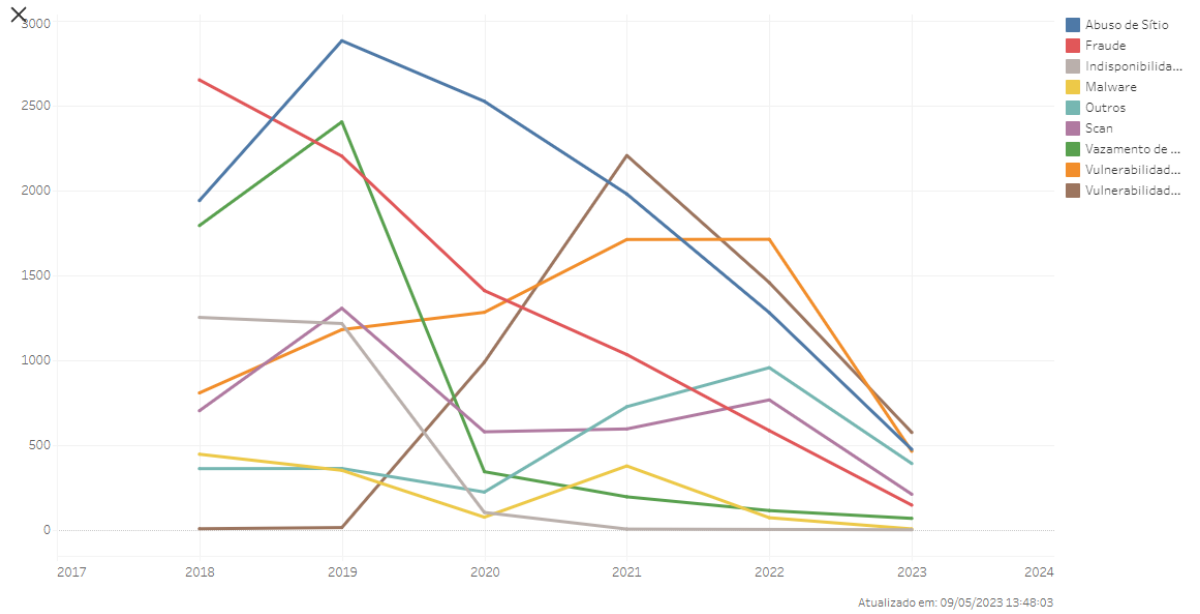


2019	2020	2021	2022	2023
23.674	24.300	22.298	18.489	8.908
10.716	5.257	4.910	3.776	1.296
1.201	2.270	3.917	3.169	1.037

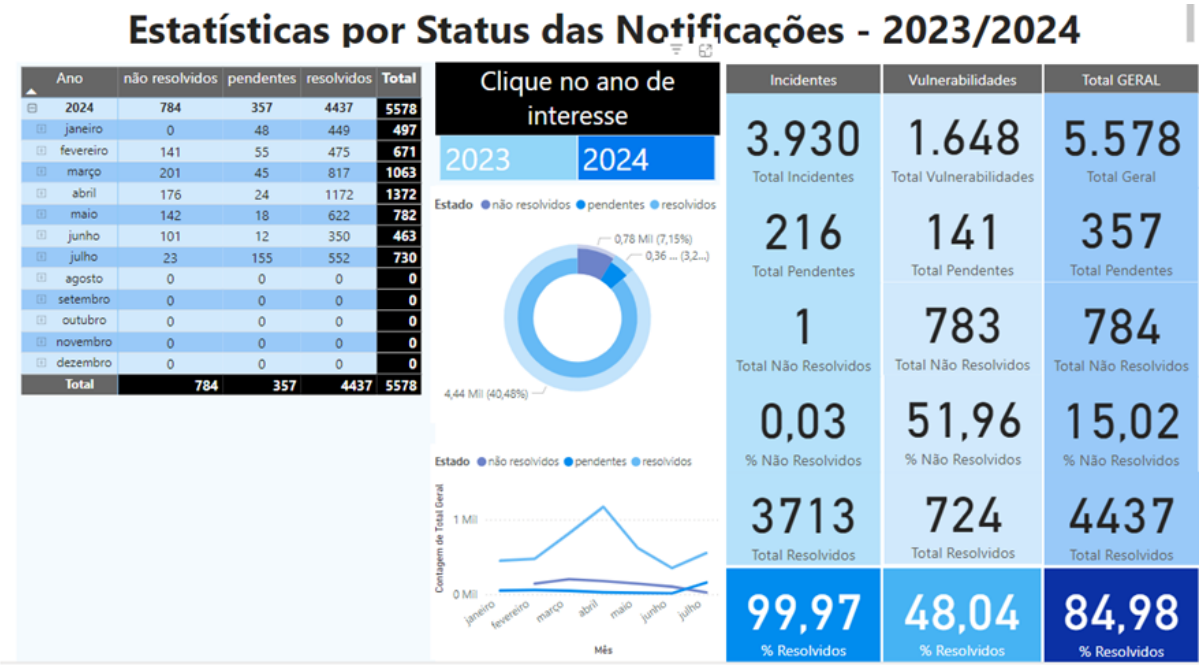
Atualizado em: 09/05/2023 13:48:03

Notificações Incidentes Vulnerabilidades

Com base nesses dados, a seguir está a Variação das Notificações por Categoria ao longo do tempo:



Para uma análise mais detalhada, apresentamos as estatísticas por status das notificações de 2023 e 2024:



Essas informações são essenciais para compreender a evolução dos incidentes cibernéticos e a efetividade das medidas de prevenção e resposta adotadas pelo CTIR Gov, permitindo uma avaliação crítica das ações implementadas e a identificação de áreas que necessitam de aprimoramento.

Adicionalmente, o Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo (CSIRT) reporta um aumento significativo no número de incidentes de segurança cibernética no âmbito do governo federal. Em 2024, o volume de incidentes já superou o total de 2023, com um registro de 3.930 incidentes até o momento.

Neste contexto, a proteção de perímetros é uma das prioridades mais relevantes para a segurança institucional. As soluções de Next Generation Firewall (NGFW) oferecem um conjunto abrangente de funcionalidades para fortalecer a segurança da rede, adaptando-se continuamente às novas ameaças e vulnerabilidades.

Atualmente, o MICD utiliza toda a arquitetura computacional de data center e perímetro compartilhada com a Funasa e com o MDR. A Funasa possui, em sua arquitetura de proteção de perímetro, um equipamento Fortinet 1801F:

Já o MDR possui uma arquitetura dividida em prédios diferentes, com um cluster de firewall no prédio 906 Norte, um cluster de firewall no Bloco E, na Esplanada dos Ministérios, e um cluster de firewall no prédio do CENAD.

O tráfego de parte do MICD, considerando usuários e serviços, está alocado no Bloco E e no 906 Norte, onde há um cluster de equipamentos Check Point Quantum 7000:

Diante da criticidade e importância desses equipamentos, especialmente aqueles com funcionalidades voltadas para a segurança da informação, é fundamental assegurar seu funcionamento contínuo e com alta resiliência. Para isso, é necessário adotar tecnologias recentes e suportadas ao longo de todo o seu ciclo de vida útil. A confiabilidade e o desempenho desejados só serão alcançados se a infraestrutura estiver atualizada, com equipamentos que não apresentem obsolescência programada e que não comprometam a operação dos sistemas. Além disso, é crucial realizar a manutenção preventiva e corretiva adequada, minimizando os riscos de interrupção dos serviços de TI.

Considerando o cenário apresentado e a necessidade de manter e racionalizar a aquisição de uma infraestrutura de segurança da informação apropriada, é imperativo garantir que essa infraestrutura tenha a capacidade necessária e ofereça serviços de suporte técnico adequados, alinhando-se à demanda atual e às projeções de crescimento para os meses e anos seguintes.

Alinhamento estratégico

O objeto da contratação está previsto no Plano de Contratações Anual 2024, conforme detalhamento a seguir:

ID PCA no PNCP: 05465986000199-0-000001/2024

Data de publicação no PNCP: 07/08/2023

Id do item no PCA: 81

Classe/Grupo: 7050 - EQUIPAMENTOS DE REDE DE TIC - LOCAL E REMOTA

Identificador da Futura Contratação: 560010-13/2024

O objeto da contratação também está alinhado com a Estratégia de Governo Digital disponível no link (https://www.gov.br /governodigital/pt-br/estrategias-e-governanca-digital/estrategianacional), e em consonância com o Plano Diretor de Tecnologia da Informação - PDTI MIDR 2023/2026 (SEI nº 4781512), aprovado pelo Comitê de Governança Digital do Ministério das Cidades, em concordância com a Nota nº 00231/2023/CONJUR-MCID, e a consulta à Secretaria de Governo Digital do MGI.

Objetivos da Estratégia Nacional de Governo Digital para o período de 2024 a 2027:

OBJETIVO	**ID**	**RECOMENDAÇÃO**
4 - PRIVACIDADE E SEGURANÇA	4.1	Instituir estrutura de governança e coordenação para implementação de medidas de reforço à privacidade, proteção de dados pessoais, segurança da informação e segurança cibernética, em articulação com estruturas de mesmo propósito de âmbito regional e nacional, em especial o Programa de Privacidade e Segurança da Informação – PPSI do governo federal.
4 - PRIVACIDADE E SEGURANÇA	4.2	Estabelecer plano de ação de reforço à privacidade, proteção de dados pessoais, segurança da informação e segurança cibernética que contemple diagnóstico, controles, metodologias e soluções tecnológicas adequadas aos riscos identificados.

Alinhamento ao Plano Diretor de Tecnologia da Informação - PDTI MIDR 2023/2026:

ALINHAMENTO AO PDTIC 2023-2026	
Id	**Ação**
NC04	Prover melhorias em soluções corporativas de TIC.
NC13	Prover soluções de segurança de TIC.
NC15	Prover infraestrutura de TIC.
A49	Adquirir Solução de Firewall.
A53	Soluções para teletrabalho seguro e gerenciável.

Motivação/Justificativa

Com a promulgação da Lei nº 14.600/2023, que deu origem ao Ministério das Cidades (MCID), mediante o desmembramento do Ministério do Desenvolvimento Regional (MDR), houve a necessidade de transferir competências e incumbências previamente atribuídas ao órgão extinto/transformado.

De acordo com o Decreto nº 11.468, de 5 de abril de 2023, o Ministério das Cidades (MCID) tem como áreas de competência os seguintes assuntos:

I - política de desenvolvimento urbano e ordenamento do território urbano;

II - políticas setoriais de habitação e de saneamento ambiental, incluídas as políticas para os pequenos Municípios e a zona rural;

III - política setorial de mobilidade e trânsito urbano;

IV - promoção de ações e programas de habitação e de saneamento básico e ambiental, incluída a zona rural;

V - promoção de ações e programas de urbanização, de desenvolvimento urbano, de transporte urbano e de trânsito;

VI - política de financiamento e subsídio ao desenvolvimento urbano, à habitação popular, ao saneamento e à mobilidade urbana;

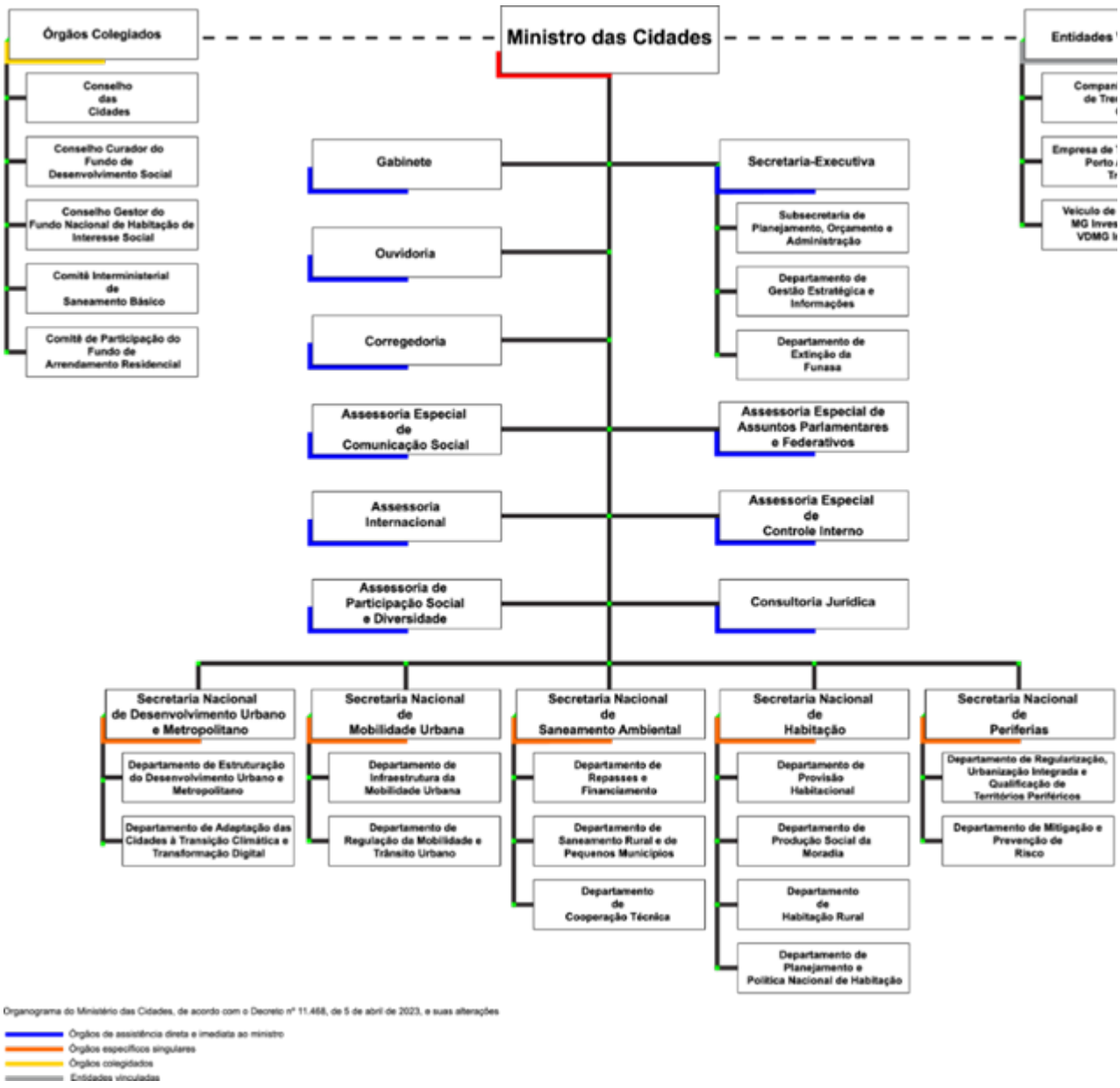
VII - planejamento, regulação, normatização e gestão da aplicação de recursos em políticas de urbanização, habitação e saneamento básico e ambiental, incluída a zona rural;

VIII - planejamento, regulação, normatização e gestão da aplicação de recursos em políticas de desenvolvimento urbano e de mobilidade e trânsito urbanos; e

IX - participação na formulação das diretrizes gerais para conservação dos sistemas urbanos de água e para adoção de bacias hidrográficas como unidades básicas do planejamento e da gestão do saneamento.

Atualmente a Estrutura Organizacional do Ministério das Cidades (MCID) compõe-se por:

ESTRUTURA ORGANIZACIONAL DO MCID



No âmbito governamental, a Tecnologia da Informação desempenha um papel fundamental na execução de políticas, no atendimento às demandas da população e na eficácia das operações.

Nesse contexto, torna-se imperativa uma seleção minuciosa de ferramentas tecnológicas que não devem apenas atender às necessidades imediatas, mas também criar um ambiente versátil, colaborativo e eficaz.

A Coordenação Geral de Tecnologia da Informação (CGTI) desempenha um papel essencial como provedor de tecnologias computacionais e sistemas de informação. Sua responsabilidade principal é oferecer soluções de informática eficientes e confiáveis, com o objetivo de aprimorar consideravelmente a qualidade dos serviços oferecidos à população. Adicionalmente, a CGTI é encarregada de gerenciar e supervisionar as iniciativas de informatização destinadas aos sistemas internos do Ministério das Cidades.

A Coordenação-Geral de Tecnologia da Informação (CGTI) é a responsável por desenvolver, aperfeiçoar, manter e dar suporte aos sistemas informatizados e aos bancos de dados no âmbito do MCID, administrando os recursos de informação e informática do órgão. Todas as áreas desse Ministério dependem de serviços específicos de Tecnologia da Informação para o desempenho de suas atividades.

As demandas da Tecnologia da Informação exigem métodos e ferramentas que garantam o nível de qualidade para atender às expectativas dos clientes e usuários, ao mesmo tempo em que acompanham a constante evolução de suas necessidades.

O presente documento analisa a contratação de uma solução composta por firewalls e suas respectivas ferramentas de gerenciamento e análise de logs, incluindo suporte e garantia. Esses ativos de segurança da informação são essenciais para a Coordenação-Geral de Tecnologia da Informação (CGTI) do Ministério das Cidades, pois permitem a gestão segura das atividades de proteção da infraestrutura contra ameaças e ataques cibernéticos, tanto da internet quanto de redes internas. Além disso, garantem acesso seguro, por meio de conexão VPN, aos servidores e colaboradores.

Atualmente, o MCID opera com uma infraestrutura de TI compartilhada com outros órgãos, como a FUNASA e o Ministério do Desenvolvimento Regional (MIDR). Cada órgão possui suas próprias particularidades e regulamentações, o que torna a situação desafiadora. A utilização de diferentes soluções de proteção de perímetro e equipes técnicas independentes dificulta a gestão de eventos de segurança e a resposta a incidentes, além de não permitir uma análise integrada dos dados.

Dessa forma, a criação de uma estrutura própria de proteção de perímetro é essencial para atender às demandas específicas do MCID, garantindo a implementação de políticas de segurança personalizadas e a proteção de dados sensíveis.

Além desta aquisição agregar tais benefícios, de acordo com a PORTARIA SGD/MGI Nº 852, DE 28 DE MARÇO DE 2023. O Programa de Privacidade e Segurança da Informação, o qual regulariza uma serie de processos e adequações em relação a privacidade e segurança da informação, esta aquisição também nos permite atender às diretrizes do PPSI como disposto no art. 3º e 4º do PPSI:

“CAPÍTULO II

DO PROGRAMA DE PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO

Art. 3º O PPSI tem como objetivo elevar a maturidade e a resiliência dos órgãos e entidades, em termos de privacidade e segurança da informação, no âmbito do SISP.

Art. 4º O PPSI caracteriza-se como um conjunto de projetos e processos distribuídos nas áreas temáticas de governança, maturidade, metodologia, pessoas e tecnologia.

§1º São iniciativas do PPSI:

I - definir e manter a estrutura de controles de privacidade e segurança da informação;

II - estabelecer e coordenar o Centro Integrado de Segurança Cibernética do Governo Digital - CISC Gov.br;

III - diagnosticar o grau de implementação dos controles de privacidade e segurança da informação pelos órgãos e entidades pertencentes ao SISP;

IV - acompanhar a implementação de controles e sensibilizar de forma contínua a Estrutura de Governança, prevista no art. 6º desta Portaria;

V - promover parcerias com órgãos e entidades públicas, entidades privadas e organismos internacionais para desenvolver e dar sustentação às iniciativas relacionadas ao tema, nos termos da legislação;

VI - promover as boas práticas por meio de disponibilização de guias, processos, modelos e procedimentos;

VII - estabelecer e coordenar o Centro de Excelência em Privacidade e Segurança da Informação do Governo Digital;

VIII - promover a cultura de privacidade e segurança da informação;

IX - apoiar na prevenção, tratamento e resposta a incidentes cibernéticos; e

X - identificar e disseminar informações sobre vulnerabilidades para a prevenção, tratamento e resposta a incidentes cibernéticos.

§2º São valores do PPSI:

I - a maturidade;

II - a resiliência;

III - a efetividade;

IV - a colaboração; e

V - a inteligência.”

Com base na proposta de implementação de uma solução integrada de proteção de rede Next Generation Firewall (NGFW) no Ministério das Cidades (MCID), é possível avaliar se as medidas do Framework do Programa de Privacidade e Segurança da Informação (PPSI) serão atendidas. Abaixo está a avaliação de cada item listado:

Avaliação das Medidas do Framework do PPSI

O órgão implementa e gerencia um firewall nos servidores?

- **Avaliação:** Com a implementação de uma solução NGFW, essa medida será atendida, garantindo a proteção adequada dos servidores.

O órgão implementa e gerencia um firewall nos dispositivos de usuário final?

- **Avaliação:** A solução deve incluir capacidades de gerenciamento de segurança para dispositivos de usuário final, embora isso possa requerer soluções adicionais específicas.

O órgão executa a gestão automatizada de patches de aplicações?

- **Avaliação**: A solução NGFW deve ser capaz de suportar a gestão de patches, mas a implementação efetiva dependerá de processos internos já existentes.

O órgão retém os logs de auditoria?

- **Avaliação**: A aquisição da NGFW incluirá a capacidade de coletar e reter logs de auditoria, atendendo a essa exigência.

O órgão coleta logs de auditoria?

- **Avaliação**: A solução deve garantir a coleta de logs de auditoria, o que é uma função central da tecnologia.

O órgão coleta logs de auditoria detalhados?

- **Avaliação**: Espera-se que a NGFW permita a coleta de logs detalhados, conforme necessário para a segurança e a conformidade.

O órgão coleta logs de auditoria de consulta DNS?

- **Avaliação**: A funcionalidade deve estar presente na NGFW, permitindo a coleta de logs de consultas DNS.

O órgão coleta logs de auditoria de requisição de URL?

- **Avaliação**: A solução deve ser capaz de coletar logs detalhados de requisições de URL, garantindo visibilidade nas atividades de navegação.

O órgão coleta logs de auditoria de linha de comando?

- **Avaliação**: A coleta de logs de linha de comando pode depender de integrações adicionais, mas a solução deve facilitar essa necessidade.

O órgão centraliza os logs de auditoria?

- **Avaliação**: A solução NGFW deve permitir a centralização dos logs, melhorando a gestão de segurança e a análise de incidentes.

O órgão coleta logs do provedor de serviços?

- **Avaliação**: Isso dependerá de acordos com os provedores de serviços, mas a solução pode ser projetada para coletar esses logs.

O órgão implanta soluções para prevenção de intrusão baseada em host?

- **Avaliação**: A NGFW pode incluir funcionalidades de prevenção de intrusão, mas a proteção baseada em host pode exigir soluções complementares.

O órgão implanta soluções para prevenção de intrusão de rede?

- **Avaliação**: A solução NGFW atenderá a essa exigência, já que é projetada para prevenir intrusões na rede.

O órgão implanta soluções de detecção e intrusão baseada em host?

- **Avaliação**: Similar ao item 2.37.1.12., pode exigir soluções adicionais para proteção baseada em host.

O órgão implanta soluções de detecção e intrusão baseada em rede?

- **Avaliação**: A NGFW atenderá a essa necessidade, proporcionando detecção e resposta a intrusões na rede.

O órgão coleta logs de fluxo e tráfego de rede?

- **Avaliação**: A solução deve incluir a coleta de logs de fluxo e tráfego, garantindo visibilidade e análise.

O órgão treina desenvolvedores em conceitos de segurança de aplicações e codificação segura?

- **Avaliação**: Essa medida depende de programas internos de treinamento, que devem ser desenvolvidos em paralelo à implementação da solução.

O órgão aplica princípios de design seguro em arquiteturas de aplicações?

- **Avaliação**: A aplicação desses princípios deve ser parte do desenvolvimento de novas aplicações e sistemas.

O órgão aproveita os módulos ou serviços controlados para componentes de segurança de aplicações?

- **Avaliação**: Essa prática deve ser incorporada nas políticas de segurança, mas dependerá de uma estratégia mais ampla.

A organização, ao realizar registros de eventos (logs), considera o princípio de minimização de dados?

- **Avaliação**: A coleta de logs deve seguir diretrizes de minimização de dados, sendo essencial para conformidade com regulamentos de proteção de dados.

Adicionalmente, é importante ressaltar que a CGTI conta atualmente com apenas cinco profissionais, todos com perfis de gestão. Portanto, a solução adquirida deve oferecer suporte completo, incluindo instalação, configuração, assistência técnica e transferência de conhecimento, para garantir uma operação eficaz.

Em resumo, a aquisição de uma solução integrada de proteção de rede NGFW permitirá ao MCID atender muitas das exigências do Framework do PPSI, especialmente em relação à proteção, monitoramento e gestão de logs de segurança. No entanto, algumas medidas exigirão a implementação de processos complementares e treinamento para garantir uma abordagem holística e eficaz à segurança da informação.

3. Área requisitante

Área Requisitante	Responsável
Coordenação de Infraestrutura da Informação - COINFRA	EMERSON MOREIRA DE MORAIS

4. Necessidades de Negócio

A crescente complexidade e interconectividade dos ambientes digitais trazem desafios significativos à segurança da informação no Ministério das Cidades (MCID). Com o aumento do tráfego de dados e a crescente dependência de serviços online, proteger informações sensíveis e garantir a continuidade das operações se tornou uma prioridade estratégica. As principais necessidades do negócio que fundamentam a solução integrada de proteção de rede *Next Generation Firewall* (*NGFW*) são as seguintes:

1. Proteção de Dados Sensíveis: O MCID lida com informações confidenciais relacionadas a políticas públicas, habitação e infraestrutura. É crucial implementar medidas robustas para proteger esses dados contra acessos não autorizados e ciberataques.

2. Continuidade das Operações: A interrupção dos serviços pode ter consequências graves para a execução de políticas públicas e o atendimento à população. Um firewall eficaz garantirá a resiliência das operações, prevenindo e respondendo rapidamente a incidentes de segurança.

3. Conformidade Regulamentar: A aquisição de uma solução integrada de proteção de rede NGFW é necessária para atender às exigências estabelecidas por legislações e normas, como a PORTARIA SGD/MGI nº 852, que regula o Programa de Privacidade e Segurança da Informação (PPSI). Cumprir essas diretrizes é crucial para assegurar a integridade e a segurança das informações.

4. Integração e Gestão de Segurança: A atual infraestrutura de TI do MCID é compartilhada com outros órgãos, o que dificulta a gestão integrada da segurança. Uma solução NGFW própria permitirá implementar políticas de segurança personalizadas e aprimorar a coordenação nas respostas a incidentes.

5. Monitoramento e Análise em Tempo Real: A capacidade de monitorar e analisar logs de segurança em tempo real é essencial para identificar rapidamente ameaças e tomar decisões informadas. Isso é fundamental para a proteção proativa da infraestrutura digital do MCID.

6. Suporte à Inovação: À medida que o MCID adota novas tecnologias e serviços online, uma solução NGFW robusta proporcionará a segurança necessária para implementar essas inovações, permitindo que o ministério se adapte às demandas emergentes sem comprometer a segurança.

7. Cultura de Segurança da Informação: A adoção de uma solução NGFW ajudará a promover uma cultura de segurança dentro do MCID, educando os colaboradores sobre a importância da proteção de dados e do uso seguro de tecnologias.

Em suma, a aquisição de uma solução integrada de proteção de rede Next Generation Firewall (NGFW) é uma necessidade crítica para o MCID. Essa solução garantirá a proteção adequada de informações sensíveis, a continuidade das operações e a conformidade com as normativas, além de preparar o ministério para enfrentar os desafios da era digital.

5. Necessidades Tecnológicas

A crescente complexidade do ambiente digital e os desafios associados à segurança da informação no Ministério das Cidades (MCID) exigem a adoção de soluções tecnológicas robustas e eficazes. As necessidades tecnológicas que fundamentam a aquisição de uma solução integrada de proteção de rede Next Generation Firewall (NGFW) incluem:

1. Capacidades Avançadas de Proteção: A solução NGFW deve oferecer funcionalidades avançadas, como inspeção profunda de pacotes, prevenção de intrusões (IPS) e filtragem de conteúdo. Essas capacidades são essenciais para detectar e bloquear ameaças em tempo real, garantindo a proteção da infraestrutura contra ataques cibernéticos.

2. Integração com Sistemas Existentes: É fundamental que a nova solução se integre harmoniosamente com a infraestrutura de TI existente, incluindo servidores, sistemas de gestão e plataformas de comunicação. Isso permitirá uma gestão centralizada e eficaz da segurança da informação.

3. Gerenciamento e Análise de Logs: A capacidade de coletar, armazenar e analisar logs de segurança é vital para identificar e responder a incidentes de forma ágil. A solução deve inc

4. Escalabilidade: A solução deve ser escalável, permitindo que o MCID amplie suas capacidades de segurança conforme a demanda por serviços e o tráfego de dados aumentem. Isso garantirá que a infraestrutura permaneça robusta diante do crescimento das operações.

5. Conectividade Segura: A implementação de conexões VPN seguras é crucial para garantir o acesso remoto de colaboradores e servidores, sem comprometer a segurança das informações. A solução NGFW deve suportar e facilitar a criação e o gerenciamento dessas conexões.

6. Facilidade de Manutenção e Atualização: A tecnologia deve ser fácil de manter e atualizar, permitindo que o MCID acompanhe a evolução do cenário de ameaças e mantenha a infraestrutura de segurança sempre alinhada às melhores práticas do setor.

7. Suporte Técnico e Treinamento: A solução deve incluir um suporte técnico robusto e programas de capacitação, possibilitando que a equipe do MCID adquira o conhecimento necessário para operar e gerenciar a solução de firewall de forma eficaz.

8. Conformidade com Normas e Regulamentações: A tecnologia escolhida deve atender às exigências das regulamentações vigentes, como as diretrizes do Programa de Privacidade e Segurança da Informação (PPSI), assegurando que o MCID permaneça em conformidade com as normas de segurança.

9. Monitoramento Contínuo: A solução deve oferecer funcionalidades de monitoramento contínuo da rede, possibilitando a detecção proativa de comportamentos anômalos e a resposta imediata a potenciais incidentes de segurança.

Essas necessidades tecnológicas são fundamentais para garantir a segurança da informação e a continuidade das operações do MCID, alinhando a infraestrutura tecnológica às exigências contemporâneas de proteção de dados e integridade operacional.

6. Demais requisitos necessários e suficientes à escolha da solução de TIC

Além dos requisitos de negócio e tecnológicos, a presente seção destaca aqueles requisitos que devem ser considerados ao longo do planejamento da contratação para assegurar o alcance dos objetivos pretendidos com a contratação, conforme a seguir.

Requisitos Legais

O presente processo de contratação deve estar aderente à Constituição Federal, à Lei nº 14.133/2021, à Instrução Normativa SGD /ME nº 94, de 2022, Instrução Normativa SEGES/ME nº 65, de 7 de julho de 2021, Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD) e a outras legislações aplicáveis;

Deve-se observar, no que couber, os seguintes normativos:

Lei 12.305/ 2010 - Institui a Política Nacional de Resíduos Sólidos;

Decreto-Lei 200/67 - Dispõe sobre a organização da Administração Federal, estabelece diretrizes para a Reforma Administrativa e dá outras providências;

Decreto nº 7.174/10 - Regulamenta a contratação de bens e serviços de informática e automação pela Administração Pública Federal;

Resolução nº 717/2019 - Aprova o Regulamento de Qualidade dos Serviços de Telecomunicações – RQUAL;

Portaria SEGES/ME nº 8.678/2021 - Dispõe sobre a Governança das Contratações Públicas no âmbito da Administração Pública federal direta, autárquica e fundacional;

Instrução Normativa SEGES/ME nº 58, de 8 de agosto de 2022 - Dispõe sobre a elaboração dos Estudos Técnicos Preliminares - ETP, para a aquisição de bens e a contratação de serviços e obras, no âmbito da administração pública federal direta, autárquica e fundacional, e sobre o Sistema ETP digital;

Instrução Normativa SEGES/ME nº 81/2022 - Dispõe sobre a elaboração do Termo de Referência - TR, para a aquisição de bens e a contratação de serviços, no âmbito da administração pública federal direta, autárquica e fundacional, e sobre o Sistema TR digital;

Portaria GSI/PR nº 120, de 21 de dezembro de 2022 - que Aprova o Plano de Gestão de Incidentes Cibernéticos para a administração pública federal;

Portaria SGD/MGI nº 852, de 28 de março de 2023 - que Dispõe sobre o Programa de Privacidade e Segurança da Informação - PPSI.

Requisitos de Manutenção

Devido às características da solução, há necessidade de realização de manutenções Preventiva e Corretiva pela Contratada, visando à manutenção da disponibilidade da solução.

Os requisitos de Manutenção seguem detalhados no item de Requisitos de Garantia, Manutenção e Assistência Técnica.

Requisitos Temporais

O prazo de vigência da contratação é de 60 (sessenta) meses contados da assinatura do contrato, prorrogável para até 10 anos, na forma dos artigos 106 e 107 da Lei n° 14.133, de 2021.

A reunião inicial de alinhamento com a Contratada, deverá ocorrer em no máximo 5 (cinco) dias corridos, posteriormente à assinatura do instrumento contratual.

A Contratada deverá iniciar a prestação dos serviços em até 30 (trinta) dias corridos após a assinatura do Contrato.

A Contratada deverá cumprir todos os prazos descritos neste Termo de Referência, respeitando os prazos máximos estabelecidos e zelando pelo cumprimento dos Níveis Mínimos de Serviço Exigidos.

O prazo de início de atendimento para os chamados de suporte técnico e manutenção pela garantia deverá estar de acordo com o especificado no acordo de nível de serviço do Termo de Referência;

O prazo de entrega e instalação deverá estar de acordo com o especificado no Termo de Referência, caso não seja especificado um prazo diferente na ordem de serviço.

Os serviços e itens a qual se refere este projeto, devem ser entregues em Brasília.

A entrega deverá acontecer no horário compreendido entre as 09:00 as 17:00 e poderá ser agendada em data e hora previamente com a CONTRATANTE;

Caberá ao CONTRATANTE rejeitar no total ou em parte, os materiais entregues em desacordo com o objeto do Termo de Referência.

O recebimento dos serviços e itens desse projeto, será efetivado pela equipe designada pelo CONTRATANTE, e dar-se-á da forma provisória e definitiva. A forma provisória será no ato da entrega dos equipamentos e a forma definitiva será após a instalação, configuração e teste da solução.

Requisitos de Segurança e Privacidade

Obedecer a todas as normas e procedimentos de segurança implementados no ambiente de TI do CONTRATANTE;

As pessoas envolvidas na execução das atividades terão acesso às instalações do CONTRATANTE por meio de credenciais emitidas pela Administração e deverão executar as atividades em ambiente definido pelo órgão, estando sujeitas, além do uso de crachás, a todas as formas de controle de acesso às dependências da instituição, tais como atendimento aos horários de expediente, vistoria de objetos que estejam portando etc.;

O acesso a áreas restritas, por técnicos das eventuais empresas CONTRATADAS, obedecerá ao previsto na POSIC do CONTRATANTE e suas Normas Complementares;

A execução das atividades deverá observar os princípios básicos de Segurança da Informação e Comunicações – SIC;

Além do que está descrito acima, deverão ser observados os requisitos de segurança e privacidade especificados nos requisitos tecnológicos da solução.

Requisitos Sociais, Ambientais e Culturais

Os serviços devem estar aderentes às seguintes diretrizes sociais, ambientais e culturais:

Requisitos Sociais, como a responsabilidade social: a contratada deve demonstrar compromisso com a responsabilidade social, cumprindo as leis trabalhistas, respeitando os direitos humanos e adotando práticas éticas de negócios e a qualidade no atendimento: a contratada deve oferecer atendimento de qualidade, com prontidão nas respostas, comunicação eficaz, empatia e respeito aos usuários.

Requisitos Ambientais: Exige-se a que os profissionais realizem o uso eficiente de energia, práticas de descarte adequadas e conformidade com regulamentações ambientais aplicáveis.

Requisitos Culturais: Conhecimento da cultura e ambiente local: Consideração da compreensão da cultura local e dos desafios específicos da região, para garantir uma adaptação adequada dos serviços de TI à realidade do Ministério das Cidades (MCID).

Sensibilidade cultural: Avaliação da capacidade das empresas licitantes em lidar com a diversidade cultural e tratar os colaboradores e usuários com respeito e igualdade, promovendo um ambiente de trabalho inclusivo.

Requisitos de Arquitetura Tecnológica

A solução ofertada deverá observar integralmente os requisitos de arquitetura tecnológica descritos no ANEXO - ESPECIFICAÇÃO TÉCNICA DOS ITENS DA SOLUÇÃO (SEI nº 5367402).

Requisitos de Projeto e de Implementação

A CONTRATADA deverá apresentar um Projeto Executivo, elaborado a partir do levantamento prévio da topologia, arquitetura e configuração atual do(s) ambiente(s) da CONTRATANTE. Esse projeto deve ser composto por um documento do tipo SOW (em tradução livre, escopo de trabalho) e conter, no mínimo, as seguintes informações:

- Objetivo;
- Plano de gerenciamento de mudanças, detalhando passo a passo o escopo da migração;
- Cronograma das atividades que serão realizadas, com os prazos estimados, considerando o cronograma de execução proposto neste Termo e as diretrizes para cada atividade;
- Projeto lógico de configuração e diagrama de interconexão dos equipamentos;
- Nome(s) do(s) gerente(s) de projeto e do(s) técnico(s) responsável(is) pela execução;
- Lista de todos os elementos instalados, contendo:
    - Nome e endereço(s) IP do equipamento;
    - Equipamento e porta na qual o equipamento foi conectado;
    - Local de instalação (prédio, andar, sala);
    - Número de série do equipamento.
- A instalação refere-se à instalação física e lógica nos locais indicados pela CONTRATANTE, abrangendo também:
    - Sua disposição e conectorização no rack de telecomunicações;
    - A instalação dos transceivers em seus módulos/slots;
    - Sua interconexão aos switches, roteadores, ADCs e servidores de rede, entre outros;
    - Suas configurações de interfaces, endereçamento e serviços de rede, além de outras configurações necessárias ou constantes no Projeto de Instalação;
    - Sua identificação e a identificação de todas as suas conexões.

O SOW deverá ser entregue pela CONTRATADA em até 10 (dez) dias úteis após a assinatura do contrato, o qual deverá ser aprovado pela CONTRATANTE. Os serviços não poderão ser iniciados antes da apresentação e assinatura de concordância de ambas as partes. O Projeto deverá ser elaborado pela CONTRATADA após a abertura da Ordem de Serviço, em tempo hábil para ser validado e aprovado pela equipe de fiscalização do contrato, considerando os prazos previstos no item de cronograma de execução.

As reuniões de controle do projeto deverão ser documentadas e registradas em ata, com as assinaturas dos presentes ou gravadas quando realizadas on-line. A data e a periodicidade de realização serão definidas em comum acordo entre as partes envolvidas no contrato.

Caberá ao Gerente de Projetos da CONTRATADA a responsabilidade por elaborar e apresentar ao CONTRATANTE os relatórios de progresso da execução contratual, bem como relatar todas as situações pertinentes à situação do projeto, incluindo a relação de atividades executadas no período, pendências e solicitações de mudança no cronograma do projeto, entre outros assuntos relacionados. Os relatórios de progresso (relatórios de acompanhamento) deverão ser disponibilizados ao CONTRATANTE em data e/ou periodicidade a ser definida em comum acordo entre as partes.

Requisitos de Implantação

A CONTRATADA deverá observar integralmente os requisitos de implantação, instalação e fornecimento descritos a seguir:

A instalação e configuração deverão ser executadas por técnicos da CONTRATADA, certificados pelo fabricante dos equipamentos fornecidos. É necessária a apresentação de documentação original que comprove a validade dessas certificações enquanto durar o contrato, podendo ser solicitada a qualquer momento.

Todos os parâmetros a serem configurados deverão ser alinhados entre as partes em reuniões de pré-projeto, que podem ser realizadas presencialmente, por telefone ou via conferência web. A CONTRATADA deverá sugerir as configurações de acordo com normas e boas práticas, cabendo à CONTRATANTE a aceitação expressa ou recusa nos casos de não atendimento às condições estabelecidas.

As configurações deverão seguir fielmente a padronização previamente estabelecida pela CONTRATANTE. A CONTRATADA deverá analisar o ambiente tecnológico atual, devendo a CONTRATANTE fornecer todas as informações necessárias sobre a infraestrutura instalada, de modo a garantir a continuidade dos serviços prestados pelo órgão durante a migração, mantendo a disponibilidade dos serviços básicos e dos demais serviços de retaguarda (aplicativos, correio eletrônico, banco de dados, Internet etc.).

A substituição da infraestrutura de firewall instalada no local deve ser planejada e executada de modo a não causar interrupções e paralisações não programadas, ou qualquer outro tipo de transtorno ao correto funcionamento do ambiente operacional da CONTRATANTE. Caso não seja possível manter a disponibilidade dos serviços básicos no momento da instalação, as manobras de implantação deverão ser realizadas durante uma janela de manutenção agendada previamente, em horários que não comprometam o funcionamento das atividades do órgão, inclusive aos sábados, domingos e feriados. Deverão ser realizadas as seguintes atividades mínimas:

- Instalação física, cabeamento e adaptações elétricas necessárias para interligação ao sistema nos datacenters da CONTRATANTE, acompanhadas e aprovadas pelas equipes técnicas responsáveis do CONTRATANTE;
- Configuração inicial do sistema, incluindo configuração de acesso de gerenciamento (usuários e senhas), configuração inicial de rede, configuração de monitoramento e ativação de licenças de criptografia e outras necessárias;
- Atualização de firmware/drivers da solução;
- Demais atividades necessárias para o perfeito funcionamento do sistema.

Todo o trabalho referente ao cabeamento, quando necessário, deverá ser realizado atendendo às normas técnicas aplicáveis, incluindo a adequada organização e identificação de cabos, segundo padrão de qualidade já existente. Todos os aspectos relacionados à adequação das condições elétricas e de rede de dados necessários à instalação dos equipamentos deverão ser levantados durante a vistoria. Durante esta etapa, as licitantes deverão avaliar os detalhes técnicos necessários ao cumprimento de suas obrigações. A adequação ao ambiente deverá englobar o fornecimento/substituição de todos os cabos, conectores, guias, leitos aramados, tomadas, abraçadeiras, velcros e demais componentes necessários à interligação de todos os produtos de hardware ofertados.

Todos os cabos e conectores fornecidos deverão ser certificados por órgãos competentes e deverão possuir o comprimento adequado para interligar todos os equipamentos fornecidos. Os equipamentos de rack deverão ser instalados nos racks disponíveis nas dependências do datacenter do CONTRATANTE. Caso haja necessidade de instalação de rack proprietário ou de adaptador para instalação em rack padrão, este deverá ser fornecido pela CONTRATADA, que providenciará todos os ajustes necessários no datacenter para que o equipamento seja devidamente instalado. Caberá à empresa CONTRATADA a conexão dos cabos aos demais equipamentos. Todo cabeamento deve ficar devidamente organizado e identificado com etiquetas apropriadas, fornecidas pela CONTRATADA.

O fornecimento de toda e qualquer ferramenta, instrumento, material e equipamento de proteção, bem como materiais complementares necessários à instalação, é de inteira responsabilidade da CONTRATADA e não deverá gerar ônus adicionais ao CONTRATANTE.

A falta de peças ou equipamentos não será considerada como alegação de força maior e não eximirá a CONTRATADA das penalidades a que estará sujeita pelo não cumprimento dos prazos estabelecidos. A CONTRATADA deverá atuar, sempre que solicitado, em qualquer movimentação de equipamentos no datacenter – entre espaços e racks, dentro do ambiente do CONTRATANTE e fora deste, conforme necessário.

A CONTRATADA deverá manter o local de execução dos serviços em perfeitas condições de limpeza e uso.

O Gerente de Projetos da CONTRATADA deverá, após a implantação da solução (instalação e configuração), entregar a documentação de “as built” em meio eletrônico, contendo todas as informações relativas à instalação e configurações realizadas, com comentários sobre os principais comandos e as justificativas das opções de parametrização, de modo a facilitar a posterior administração da solução e a continuidade de seu funcionamento.

Deverá constar da documentação de “as built” todas as informações do Projeto Executivo atualizadas, como a localização física no datacenter da CONTRATANTE, conexões físicas utilizadas, endereços IP e nomenclaturas, onde deverão ser demonstradas as velocidades e a qualidade da transmissão de dados.

A entrega da documentação de “as built” sinaliza a conclusão da etapa de implantação, solicitando a validação para fins de recebimento definitivo. Esta documentação também deverá conter fotos do ambiente instalado, assim como, se necessário, imagens ilustrativas de configurações.

Requisitos de Garantia, Manutenção e Assistência Técnica

O prazo de garantia contratual dos bens, complementar à garantia legal, é de, no mínimo, 60 (sessenta) meses, ou pelo prazo fornecido pelo fabricante, se superior, contado a partir do primeiro dia útil subsequente à data do recebimento definitivo do objeto.

A garantia será prestada com o objetivo de manter os equipamentos e itens de software fornecidos em perfeitas condições de uso, sem qualquer ônus ou custo adicional para o CONTRATANTE.

A garantia abrange a realização da Manutenção Preventiva e Corretiva dos bens, realizada pelo próprio CONTRATADO ou, se for o caso, por meio de assistência técnica autorizada, de acordo com as normas técnicas específicas.

Entende-se por Manutenção Preventiva os serviços que compreendem verificações frequentes em relação ao bom funcionamento do hardware e à atualização de drivers, softwares e firmwares necessários para todos os itens que compõem os equipamentos. Quando necessário, haverá a substituição de peças e componentes, que deverão ser novos, originais e não recondicionados. Os serviços deverão ser realizados mediante cronograma de execução previamente aprovado pelo CONTRATANTE.

As verificações preventivas ocorrerão pelo menos trimestralmente, em datas a serem definidas pelo CONTRATANTE. A manutenção preventiva poderá ser solicitada pela CONTRATANTE, que definirá o nível de severidade, por meio de chamado registrado junto à CONTRATADA.

A CONTRATADA deverá emitir um relatório de atendimento de manutenção preventiva, que deverá evidenciar os parâmetros de desempenho do equipamento, as versões de software e as recomendações, quando for o caso.

Uma vez identificados vícios ou defeitos nos equipamentos, a CONTRATADA deve prover todas as manutenções corretivas necessárias para a normalização do ambiente, corrigindo todos os defeitos, mensagens de erro ou qualquer tipo de mau funcionamento apresentado em qualquer um dos equipamentos e seus componentes internos.

Entende-se por Manutenção Corretiva aquela destinada a corrigir os defeitos apresentados pelos bens, compreendendo a substituição de peças, a realização de ajustes, reparos, atualizações e correções necessárias.

As peças que apresentarem vício ou defeito no período de vigência da garantia deverão ser substituídas por outras novas, de primeiro uso e originais, que apresentem padrões de qualidade e desempenho iguais ou superiores aos das peças utilizadas na fabricação do equipamento, sem custo adicional para o CONTRATANTE.

Uma vez notificado, o CONTRATADO realizará a reparação ou substituição dos bens que apresentarem vício ou defeito no prazo máximo de 1 (um) dia útil, contados a partir da data de retirada do equipamento das dependências da Administração pelo CONTRATADO ou pela assistência técnica autorizada.

O prazo indicado no subitem anterior poderá ser prorrogado uma única vez, por igual período, mediante solicitação escrita e justificada do CONTRATADO, aceita pelo CONTRATANTE.

Na hipótese do subitem acima e seu predecessor, o CONTRATADO deverá disponibilizar equipamento equivalente, de especificação igual ou superior ao anteriormente fornecido, para utilização em caráter provisório pelo CONTRATANTE, de modo a garantir a continuidade dos serviços e trabalhos administrativos durante a execução dos reparos.

Decorrido o prazo para reparos e substituições, ou violados os NÍVEIS MÍNIMOS DE SERVIÇO, sem o atendimento da solicitação do CONTRATANTE ou a apresentação tempestiva de justificativas pelo CONTRATADO, fica o CONTRATANTE autorizado a contratar empresa diversa para executar os reparos, ajustes ou a substituição do bem ou de seus componentes, bem como a exigir do CONTRATADO o reembolso pelos custos respectivos, sem que tal fato acarrete a perda da garantia dos equipamentos. O custo referente ao transporte dos equipamentos cobertos pela garantia será de responsabilidade do CONTRATADO.

A garantia legal ou contratual do objeto tem prazo de vigência própria e desvinculado daquele fixado no contrato, permitindo a eventual aplicação de penalidades em caso de descumprimento de alguma de suas condições, mesmo depois de expirada a vigência contratual.

Dos requisitos específicos de assistência técnica:

Este serviço compreende o apoio técnico à distância e/ou presencial (on-site) fornecido pela assistência técnica do fabricante dos equipamentos e da CONTRATADA para solucionar problemas de ordem sistêmica, problemas em equipamentos desta marca e problemas decorrentes de mau funcionamento de software, bem como solucionar dúvidas quanto à correta operação e configuração dos equipamentos.

Deverá existir acesso ao serviço de assistência técnica do fabricante e da CONTRATADA por telefone gratuito, e-mail ou acesso seguro ao site, 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana. No site do fabricante, deverão existir ferramentas de autosserviço que permitam o diagnóstico e sugestões de solução do problema, quando possível.

Deverá existir acesso ao serviço de assistência técnica da CONTRATADA, por telefone gratuito, e-mail ou acesso ao site, 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana. A indisponibilidade da comunicação por parte da CONTRATADA não afetará a contagem de tempo relativa aos prazos de atendimento.

Os chamados junto à CONTRATADA deverão ser atendidos por profissionais da CONTRATADA, em português, e serão usados para abrir solicitações de informações, reportar incidentes ou esclarecer dúvidas quanto à utilização dos produtos e soluções fornecidos.

Dos requisitos específicos de acesso à documentação:

Este serviço compreende o acesso remoto, por parte da CONTRATANTE, às documentações técnicas dos equipamentos do fabricante.

A CONTRATANTE deverá ter acesso direto à base de dados de conhecimento do fabricante dos equipamentos, que contenha especificações técnicas, informações, assistência e orientação para instalação, desinstalação, configuração e atualização de firmware e software, aplicação de correções (patches), diagnósticos, avaliações e resolução de problemas, além de demais atividades relacionadas à correta operação e funcionamento dos equipamentos.

Dos requisitos específicos de garantia técnica do fabricante:

A CONTRATADA deverá descrever, em sua proposta, os termos da garantia técnica oferecida pelo fabricante, incluindo o Part Number da garantia ofertada e fornecendo também, em momento oportuno, o número de contrato individual (em nome da CONTRATANTE) junto ao fabricante.

O Termo de Garantia Técnica terá duração mínima de 60 (sessenta) meses.

Dos requisitos de reposição de equipamento defeituoso:

Este serviço compreende o envio de equipamento(s), componente(s), acessório(s) e dispositivo(s) novos, de primeiro uso e de modelo igual ou superior ao(s) danificado(s), às expensas do fabricante, às dependências da CONTRATANTE.

O contrato de reposição de equipamento, peças ou acessórios deverá ser na modalidade 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, devendo o equipamento substituto (definitivo ou provisório) ser entregue na CONTRATANTE até o próximo dia útil (Next Business Day - NBD) após a abertura do chamado.

Para determinação do horário de início de cada chamado referente à substituição de equipamento defeituoso, devem ser levadas em consideração as seguintes condições: caso a determinação de falha do hardware pelo fabricante tenha ocorrido antes das 15h, horário local de Brasília-DF, de segunda a sexta-feira (excluindo os feriados), o equipamento deverá ser enviado no mesmo dia para chegar no próximo dia útil. Para as solicitações feitas depois das 15h, o fabricante deverá entregar o equipamento substituto até o segundo dia útil após a determinação da falha.

O equipamento substituto passará à propriedade da CONTRATANTE, devendo ser imediatamente incluído no contrato de manutenção vigente em substituição ao equipamento danificado. O equipamento substituído deverá ser devolvido ao fabricante às expensas do mesmo, em até 5 (cinco) dias úteis.

A CONTRATANTE deverá ter acesso à Central de Assistência Técnica (TAC) do fabricante para abertura dos chamados, bem como para acompanhar e gerenciar os casos quando necessário. Esse acesso deverá ser provido 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, através de login/senha individual. A CONTRATANTE deverá ter a opção de abrir os chamados junto ao fabricante com o intermédio da CONTRATADA.

Os requisitos de Garantia, Manutenção e Assistência Técnica deverão observar os NÍVEIS MÍNIMOS DE SERVIÇO exigidos, descritos no capítulo Modelo de Gestão de Contrato deste Termo.

Requisitos de Experiência Profissional

Os serviços de Garantia, Manutenção e Assistência Técnica deverão ser prestados por técnicos devidamente capacitados nos produtos em questão, bem como com todos os recursos ferramentais necessários para a prestação dos serviços.

A CONTRATADA deverá possuir equipe qualificada para realizar:

- A instalação e configuração dos equipamentos e/ou licenças de software previstos na presente contratação;
- A execução da assistência técnica, manutenção e garantia, nos casos em que deverá efetuar manutenção corretiva, cobrindo todo e qualquer defeito apresentado, incluindo o fornecimento e a substituição de peças e/ou componentes, ajustes, reparos e correções necessárias, quando for o caso.

Outros requisitos estão estabelecidos nos itens de requisitos de Garantia, Manutenção e Assistência Técnica e de Qualificação Técnica para Habilitação.

Requisitos de Formação da Equipe

Os serviços deverão ser prestados por técnicos devidamente capacitados.

Todos os recursos humanos necessários à realização das atividades de instalação e configuração da solução estão sob responsabilidade da CONTRATADA e serão supervisionados pela CONTRATANTE.

Deverá ser apresentado um Preposto, nos termos do art. 118 da Lei 14.133/2021, aceito pela Administração, para representar a CONTRATADA ao longo da execução do contrato.

Deverá ser apresentado um Gerente de Projetos (podendo este ser o Preposto), que será o ponto focal para tratativas de assuntos relativos à execução dos serviços, sendo responsável por coordenar e orientar todos os técnicos na execução dos serviços, de forma que os prazos e a qualidade estabelecidos sejam respeitados. Caberá ainda ao Gerente de Projetos apresentar na reunião uma lista de contatos para comunicação, a fim de esclarecer dúvidas ou oferecer apoio em itens relacionados ao projeto.

Requisitos de Metodologia de Trabalho

O fornecimento dos equipamentos está condicionado ao recebimento, pelo CONTRATADO, de uma Ordem de Serviço ou de Fornecimento de Bens (OSFB) emitida pela CONTRATANTE. A OSFB indicará o tipo de equipamento, a quantidade e a localidade onde os equipamentos deverão ser entregues. O CONTRATADO deve fornecer meios digitais para contato e registro de ocorrências relacionadas aos serviços de Garantia, Manutenção e Assistência Técnica, com funcionamento 24 (vinte e quatro) horas por dia e 7 (sete) dias por semana.

O andamento do fornecimento dos equipamentos deverá ser acompanhado pelo CONTRATADO, que dará ciência à CONTRATANTE sobre eventuais acontecimentos. A CONTRATANTE será responsável pela condução da metodologia de trabalho. A CONTRATADA deverá adotar as boas práticas e técnicas conhecidas de gerenciamento de projeto.

Os produtos e/ou serviços deverão ser entregues no endereço indicado no item de “Entrega”, em prazo não superior ao que for definido neste Termo. Os equipamentos e as licenças de software serão instalados e configurados pela equipe técnica da CONTRATADA.

Os Fiscais Técnico e Requisitante emitirão um Termo de Recebimento Provisório quando da entrega do objeto resultante de cada Ordem de Serviço ou de Fornecimento de Bens. Após a instalação e configuração dos equipamentos e/ou softwares e das respectivas licenças pela CONTRATADA, e após a análise da qualidade e verificação da aderência aos termos contratuais pelos Fiscais e pelo Gestor do Contrato, o CONTRATANTE emitirá um Termo de Recebimento Definitivo dos produtos.

O recebimento provisório ou definitivo do objeto não exclui a responsabilidade da CONTRATADA pelos prejuízos resultantes da incorreta execução do contrato. Será realizado o acompanhamento do contrato pela Equipe de Gestão e Fiscalização Contratual, inclusive nos casos de necessidade de manutenção e garantia da CONTRATADA.

O não cumprimento dos prazos exigidos ensejará sanções previstas no Termo de Referência.

Requisitos de Segurança da Informação e Privacidade

Os serviços contratados deverão ser prestados em conformidade com leis, normas e diretrizes vigentes no âmbito da Administração Pública Federal relacionadas à Segurança da Informação e Comunicações (SIC) – em especial atenção à Lei Federal n° 13.709/2018 (LGPD).

A CONTRATADA deverá adotar a POSIC do órgão, e as normas relativas a Segurança da Informação do Governo Federal.

A CONTRATADA deverá credenciar junto à CONTRATANTE todos os seus profissionais que venham a ser designados para prestar serviços, independentemente do formato de execução (presencial, remoto e/ou híbrido).

A CONTRATADA deverá adotar critérios adequados para o processo seletivo dos profissionais que irão atuar diretamente na execução do objeto, com o propósito de evitar a incorporação de perfis que possam comprometer a segurança ou credibilidade da CONTRATANTE.

A CONTRATADA deverá comunicar à CONTRATANTE, com a antecedência mínima necessária, qualquer ocorrência de transferência, remanejamento ou demissão de funcionários envolvidos diretamente na execução do Contrato para que seja providenciada a imediata revogação de todos os privilégios de acesso aos sistemas, informações e recursos da CONTRATANTE porventura colocados à disposição para realização dos serviços contratados.

Conforme aplicável para a característica dos serviços contratados, a CONTRATADA deve garantir que sua equipe profissional seja treinada, qualificada e esteja disponível para executar os serviços atribuídos.

Todos os funcionários da Empresa CONTRATADA envolvidos na prestação dos serviços deverão utilizar crachá.

Todas as informações as quais a CONTRATADA tiver acesso em função da execução dos serviços deverão ser tratadas como confidenciais, sendo vedada sua reprodução, utilização ou divulgação a terceiros.

Os representantes, empregados e colaboradores da CONTRATADA deverão zelar pela manutenção do sigilo de dados, informações, documentos e especificações técnicas, que tenham conhecimento em razão dos serviços executados.

A CONTRATADA deverá adotar todas as medidas necessárias para assegurar a disponibilidade, integridade, confidencialidade e autenticidade das informações a serem tratadas no âmbito da prestação dos serviços.

A CONTRATADA deverá implementar medidas para garantir a proteção dos dados, antecipando ameaças à privacidade, à segurança e à integridade, prevenindo acesso não autorizado às informações disponibilizadas para prestação dos serviços.

A CONTRATADA não pode obter, capturar, copiar ou transferir qualquer tipo informação de propriedade da CONTRATANTE, sem autorização.

A CONTRATADA deverá submeter-se aos procedimentos contidos nas normas de segurança corporativa do Ministério das Cidades (MCID) e da Administração Pública em todos os eventos em que for necessária a presença de seus prepostos e/ou funcionários nas dependências do órgão.

A CONTRATADA não poderá se utilizar da presente contratação para obter qualquer acesso não autorizado às informações de propriedade do CONTRATANTE.

A CONTRATADA deverá identificar qualquer equipamento de sua propriedade que venha a ser instalado nas dependências do CONTRATANTE, utilizando placas de controle patrimonial, selos de segurança etc.

A CONTRATADA deverá assinar o Termo de Compromisso, e seus funcionários alocados na prestação de serviços, o Termo de Ciência.

A Contratada deverá conhecer todas as normas, políticas e procedimentos de segurança estabelecidos pelo Ministério das Cidades para execução do Contrato.

Não será permitido, salvo justificado, que o ambiente seguro seja acessado por pessoas além daquelas necessárias para a prestação de serviços do objeto contratado.

O acesso dos profissionais da Contratada às dependências do Ministério das Cidades estará sujeito às suas normas referentes à identificação (crachá funcional), trajes, trânsito e permanência em suas dependências.

A Contratada responsabilizar-se-á integral e solidariamente pelos atos praticados de seus empregados e/ou prestadores de serviço nas dependências do Ministério das Cidades ou mesmo fora delas, que venham a causar danos ou colocar em risco o patrimônio do Ministério.

A solução deverá atender aos princípios e procedimentos elencados na Política de Segurança da Informação do Contratante.

A CONTRATADA deverá manter sigilo absoluto sobre quaisquer dados, informações, artefatos, contidos em quaisquer documentos e em quaisquer mídias de que venha a ter conhecimento durante a execução dos trabalhos, não podendo, sob qualquer pretexto divulgar, reproduzir ou utilizar, sob as penas da lei, independentemente da classificação de sigilo conferida a tais documentos.

A CONTRATADA não poderá divulgar quaisquer informações a que tenha acesso em virtude dos trabalhos a serem executados ou de que tenha tomado conhecimento em decorrência da execução do objeto, sem autorização, por escrito, sob pena de aplicação das sanções cabíveis, além do pagamento de indenização por perdas e danos.

Cada profissional da CONTRATADA deverá assinar termo de responsabilidade e sigilo, comprometendo-se a não divulgar nenhum assunto tratado nas dependências da CONTRATANTE ou a serviço deste, salvo se expressamente autorizado.

Cada profissional da CONTRATADA deverá assinar termo de compromisso declarando total obediência às normas de segurança vigentes, ou que venham a ser implantadas, a qualquer tempo.

Sustentabilidade

Devem ser atendidos os seguintes requisitos de sustentabilidade, conforme estabelecido no Guia Nacional de Contratações Sustentáveis:

Só será admitida a oferta de Next Generation Firewall(NGFW) que cumpra os critérios de segurança, compatibilidade eletromagnética e eficiência energética, previstos na Portaria nº 304, de 2023 do INMETRO.

Indicação de marcas ou modelos (Art. 41, inciso I, da Lei nº 14.133, de 2021):

Na presente contratação, não será admitida a indicação da marca/fabricante;

Da exigência de carta de solidariedade

Em caso de fornecedor revendedor ou distribuidor, não será exigida carta de solidariedade emitida pelo fabricante, que assegure a execução do contrato.

Subcontratação

Não é admitida a subcontratação do objeto contratual.

Da verificação de amostra do objeto

Não será exigida a verificação de amostra do objeto

Garantia da Contratação

Será exigida a garantia da contratação a que se referem os arts. 96 e seguintes da Lei nº 14.133, de 2021, no percentual e nas condições descritas nas cláusulas do contrato.

Em caso de opção pelo seguro-garantia, a parte adjudicatária deverá apresentá-lo, no máximo, até a data de assinatura do contrato.

A garantia, nas modalidades caução e fiança bancária, deverá ser prestada em até 10 dias úteis após a assinatura do contrato.

O CONTRATANTE poderá utilizar o valor da garantia prestada para descontar os valores referentes a eventuais glosas e multas aplicadas à CONTRATADA, além da satisfação de prejuízos causados ao CONTRATANTE ou a terceiros na execução do objeto contratual por culpa ou dolo da CONTRATADA.

Se o valor da garantia, ou parte dele, for utilizado em pagamento de qualquer obrigação ou em decorrência de penalidade imposta, inclusive indenização a terceiros, a CONTRATADA se obriga a efetuar a respectiva reposição ou complementação no prazo de 10 (dez) dias úteis, a contar da data do recebimento da comunicação feita pelo CONTRATANTE.

Caso a CONTRATADA não cumpra o disposto nos itens anteriores dentro do prazo estipulado, ficará sujeita às penalidades contratuais cabíveis.

Em caso de aditamento do contrato, por motivos previstos na Lei, a CONTRATADA fica obrigada a apresentar garantia complementar ou substituí-la, no mesmo percentual e nas modalidades constantes desta Seção.

O contrato poderá oferecer maior detalhamento das regras que serão aplicadas em relação à garantia da contratação.

Informações relevantes para o [dimensionamento E/OU apresentação] da proposta

A proposta de preços deverá ser apresentada com descrição detalhada do objeto ofertado, devendo estar de acordo com as quantidades, especificações técnicas e condições estabelecidas no Termo de Referência e no Edital.

A proposta técnica de preços deverá ter prazo de validade não inferior a 60 (sessenta) dias corridos, a partir da data da sessão pública.

A licitante deverá declarar, no momento de sua proposta, que possui capacidade técnica adequada para executar o objeto da licitação atendendo aos critérios de qualidade e aos níveis de serviço exigidos, cumprindo os requisitos especificados para a presente contratação.

A proposta deverá ser redigida em Língua Portuguesa (pt-BR), salvo quanto às expressões técnicas de uso corrente, sem emendas, rasuras ou entrelinhas, devidamente datada, sendo clara e precisa, sem alternativas de preços ou qualquer outra condição que induza o julgamento a ter mais de um resultado, com todos os preços expressos em REAIS (R$) e declaração expressa de que os serviços ofertados atendem aos requisitos técnicos especificados no Termo de Referência.

7. Estimativa da demanda - quantidade de bens e serviços

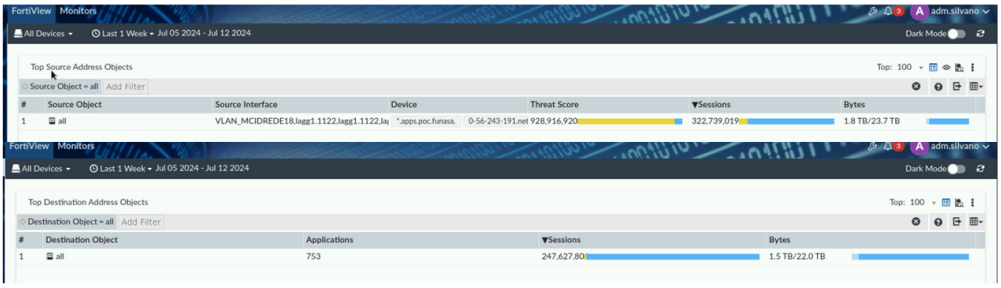
ESTIMATIVA DA DEMANDA - QUANTIDADE DE BENS E SERVIÇOS

Coleta e Análise de Dados

Para dimensionar adequadamente os equipamentos, foram realizadas as seguintes etapas:

- **Monitoramento de Tráfego no Fortinet:** O tráfego de entrada (TX) e saída (RX) foi monitorado diretamente nas interfaces ativas do equipamento Fortinet. A análise envolveu registros que foram documentados em um sistema específico (SEI nº 5340643).
- **Arquitetura do MIDR e CPSizement:** Para o Check Point, foi utilizado o processo de CPSizement (disponível em https://support.checkpoint.com/results/sk/sk88160), que envolveu a coleta de tráfego do firewall do MIDR durante um período de 7 dias. Essa coleta considerou os dois principais sites do MIDR: Bloco E e 906 Norte.

Segue em anexo o relatório detalhado do tráfego do firewall FGT-1801F da Funasa:



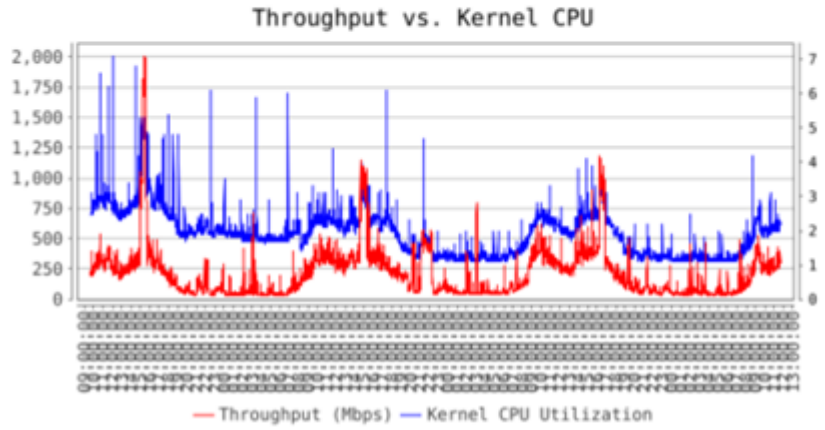
Essa coleta resultou no cenário a seguir, considerando os dois sites do MIDR: Bloco E e 906 Norte:

Bloco E:

Traffic Characteristics (Measured)	
Max. Throughput	2070.245320
Max. Packet Rate	201007
Max. Concurrent Connections	43726
Number of Internal IPs	3458
Average Percent of Accelerated Packets	94.19%
Average Percent of VPN Traffic	1.47%

Resource Utilization (Measured)	
Max CPU	17%
Max Kernel CPU	10%
Max. Memory	22150020 KB
Detected Interface Packet Drops	no
Install Policy During Script Execution	yes

Traffic vs. CPU Performance Graph

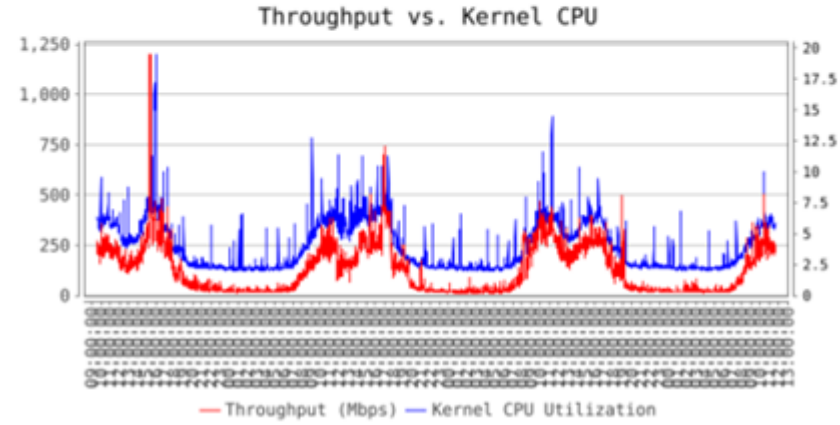


906 Norte:

Traffic Characteristics (Measured)	
Max. Throughput	1228.664011
Max. Packet Rate	129410
Max. Concurrent Connections	85657
Number of Internal IPs	2674
Average Percent of Accelerated Packets	84.45%
Average Percent of VPN Traffic	0.08%

Resource Utilization (Measured)	
Max CPU	63%
Max Kernel CPU	21%
Max. Memory	8962736 KB
Detected Interface Packet Drops	no
Install Policy During Script Execution	yes

Traffic vs. CPU Performance Graph



Resultados da Análise

Os resultados obtidos indicam um volume médio de tráfego em torno de **4 Gbps**, levando em conta apenas as funcionalidades de NGFW. Esses números não incluem a capacidade de prevenção de ameaças de dia zero e a inspeção de tráfego SSL. O volume de processamento alcançou:

- 400.000 pacotes por segundo;
- Mais de 500.000 novas conexões por segundo.

Projeção de Crescimento

Considerando o relatório apresentado de quantidade de sessões atuais do firewall utilizado apresentando no quadro abaixo, e considerando que temos uma projeção de crescimento inclusive de usuários apresentados no processo da CGGP (80000.012620 /2023-25), e que este seria um projeto de 60 (sessenta) meses.

Traffic Statistics

#	Summary	Statistics
1	Total Sessions	633,496,910
2	Total Bytes Transferred	26,817.20GB
3	Most Active Date By Sessions	2024-07-09
4	Total Users	208,616
5	Total Applications	90,439
6	Total Destinations	97,998
7	Average Sessions Per Day	90,499,559
8	Average Bytes Per Day	3,831.03GB

É essencial prever um crescimento em conformidade não só com número de usuários mas sim em conformidade com sessões, transferência de bytes, aplicações, número de conexões VoIP, número de transmissões de vírus detectadas, número de solicitações de proxy HTTP processadas, número de conexões de proxy SMTP atuais, contagem de sessões do sistema, ou seja tudo que precisa ser monitorado, desta forma uma projeção de crescimento de 10% ao ano em cinco anos seria um crescimento de 50% ao longo dos próximos cinco anos, sabemos que isso é uma estimativa e contando que esse crescimento é estimativo consideramos 30% de crescimento como razoabilidade de atendimento a este ministério uma vez que os serviços de TIC são crescentes, desta forma para atender a essa demanda de forma eficiente, os equipamentos devem ter uma capacidade mínima de:

- **10 Gbps de throughput** para as funcionalidades de NGFW.

Entretanto, ao considerar a evolução natural das tecnologias e a necessidade de incluir funcionalidades adicionais, a demanda identificada é:

- **25 Gbps de throughput** para o processamento do tráfego de usuários, com funcionalidades de NGFW habilitadas (incluindo IPS e controle de aplicações).
- **15 Gbps de throughput** para Threat Protection, incorporando IPS, Antivírus/Anti-Malware, controle de Aplicação e Filtragem de URL.

Quantidade de bens e serviços

Para atendimento às necessidades elencadas, a solução prevista nesta contratação consiste nos seguintes itens:

ITEM	DESCRIÇÃO	SUB-DESCRIÇÃO	UNIDADE DE MEDIDA	QUANTIDADE
1	Solução de segurança em Cluster para proteção avançada de perímetro - Firewall - denominada Next Generation Firewall(NGFW) com suporte, garantia e licenciamento inclusos para 60 meses com repasse de conhecimento.	Hardware /Licenciamento	Unidade	4
2	Solução para Gerenciamento de LOGS e Automação		Unidade	1
3	Solução para Gerenciamento Centralizado de NGFW		Unidade	1
4	Instalação e Configuração		Unidade	1

Da Solução de segurança em Cluster - denominada Next Generation Firewall(NGFW)

A solução proposta, com dois clusters de firewall, cada um com duas unidades, garante a alta disponibilidade e a escalabilidade necessárias para atender às demandas do Ministério das Cidades. Essa arquitetura redundante distribui a carga de trabalho, otimiza o desempenho e minimiza o risco de interrupções no serviço. Além disso, a solução oferece a flexibilidade necessária para acompanhar o crescimento da rede e as mudanças no cenário de ameaças, proporcionando uma proteção robusta e adaptável aos desafios da segurança cibernética.

Do Licenciamento da solução

A necessidade de adquirir 4 licenças para os equipamentos NGFW se justifica pela arquitetura da solução em cluster, que exige um licenciamento individual para cada dispositivo. Essa configuração garante a alta disponibilidade, a redundância e o equilíbrio de carga na rede, proporcionando uma segurança mais robusta e eficiente.

Justificativa para a Contratação dos Componentes Adicionais

A inclusão dos componentes de **Gerenciamento de Logs e Automação**, **Gerenciamento Centralizado** e **Instalação e Configuração** à solução de firewall em cluster proporciona um conjunto de benefícios que vão além da simples proteção do perímetro, garantindo uma segurança mais robusta e eficiente para o Ministério das Cidades.

Gerenciamento de Logs e Automação:

- **Visibilidade aprofundada:** Permite uma análise detalhada dos eventos de segurança, identificando padrões, correlacionando incidentes e detectando ameaças emergentes de forma proativa.
- **Geração de relatórios personalizados:** Possibilita a criação de relatórios customizados para atender às necessidades específicas de cada área, facilitando a tomada de decisões e o cumprimento de requisitos regulatórios.
- **Automação de respostas:** Permite a automação de tarefas repetitivas, como a geração de alertas e a aplicação de medidas corretivas, reduzindo o tempo de resposta a incidentes e minimizando o risco de falhas humanas.
- **Compliance:** Auxilia no cumprimento de normas e regulamentações, como a LGPD, fornecendo as evidências necessárias para auditorias e investigações.

Gerenciamento Centralizado:

- **Consolidação da gestão:** Permite gerenciar todos os firewalls da organização a partir de um único console, simplificando as operações e reduzindo a complexidade da gestão da segurança.
- **Visão holística:** Oferece uma visão unificada da segurança da rede, facilitando a identificação de vulnerabilidades e a avaliação do risco.
- **Otimização de recursos:** Permite otimizar a configuração dos firewalls, garantindo a utilização eficiente dos recursos e maximizando o desempenho.

Instalação e Configuração:

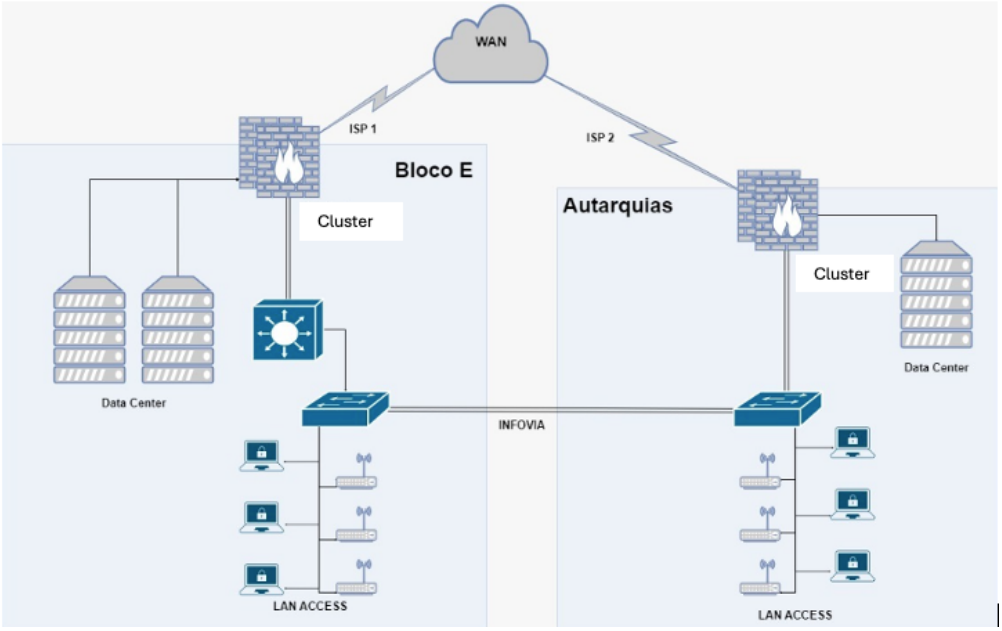
- **Garantia da correta implementação:** Assegura que a solução seja instalada e configurada de acordo com as melhores práticas, maximizando a eficácia da proteção.
- **Otimização do desempenho:** Permite ajustar a configuração dos firewalls para obter o melhor desempenho possível, considerando as características da rede e os requisitos de segurança.
- **Redução de riscos:** Minimiza o risco de erros de configuração que possam comprometer a segurança da rede.

Estruturação dos Equipamentos

Com base na topologia sugerida e na quantidade de prédios atendidos pelo MCID, foram estipuladas as seguintes necessidades:

- **Clusters de Firewall:**
    - **Bloco E:** Um cluster formado por dois equipamentos de firewall (2 unidades).
    - **Setor de Autarquias:** Um cluster adicional também com dois equipamentos de firewall (2 unidades).

Portanto, para atender a estas demandas, o licenciamento total necessário será de **4 unidades de firewall**, formando dois clusters que garantam a redundância e a continuidade das operações, conforme desenho da topologia sugerido abaixo:



A solução proposta, com base na topologia sugerida e no dimensionamento dos equipamentos, oferece uma proteção robusta e escalável para a rede do Ministério das Cidades. A arquitetura em cluster, a redundância dos equipamentos e a flexibilidade da solução garantem a segurança e a disponibilidade dos serviços, atendendo às necessidades específicas do órgão.

LEVANTAMENTO DE SOLUÇÕES

As alternativas apresentadas estão apresentadas no item "9: Análise Comparativa de Soluções", que a seguir elenca os principais pontos positivos e negativos de cada solução ou cenário considerado para atender à demanda. Serão avaliados os seguintes cenários e soluções:

Solução 1 - Renovação do contrato atual;

Solução 2 – Utilização de software livre;

Solução 3 – Contratação de uma suíte de soluções de proteção avançada de perímetro.

8. Levantamento de soluções

LEVANTAMENTO DE SOLUÇÕES

As alternativas apresentadas estão apresentadas no item "9: Análise Comparativa de Soluções", que a seguir elenca os principais pontos positivos e negativos de cada solução ou cenário considerado para atender à demanda. Serão avaliados os seguintes cenários e soluções:

Solução 1 - Renovação do contrato atual;

Solução 2 – Utilização de software livre;

Solução 3 – Contratação de uma suíte de soluções de proteção avançada de perímetro.

9. Análise comparativa de soluções

A equipe de planejamento procurou avaliar as opções disponíveis e, por fim, determinar o melhor modelo de fornecimento do produto. Com base nessas informações, foram analisados todos os prós e contras das alternativas resultantes das análises anteriores, comparando-as com a demanda identificada pela Área Requisitante. Isso permitiu concluir qual cenário atende de forma mais eficiente às necessidades.

Nesse contexto, a equipe de planejamento da contratação entende que a plataforma tecnológica objeto do presente estudo deve ser baseada nos pilares tecnológicos elencados abaixo. Essa orientação tem como objetivo estabelecer as características fundamentais da solução, de modo a permitir a contratação de uma solução de proteção avançada de perímetro.

Para o levantamento das soluções disponíveis que possam atender às necessidades da contratação (alinhado ao inciso II do art. 11 da Instrução Normativa SGD/ME nº 94, de 23 de dezembro de 2022) foram consideradas as possibilidades descritas abaixo:

a) **necessidades similares em outros órgãos ou entidades da Administração Pública e as soluções adotadas** (IN/SGD/ME nº 94/2022 Art. 11, II, a)

A verificação da disponibilidade de soluções similares em outros órgãos ou entidades da Administração Pública foi conduzida principalmente por meio de consulta à base de dados do Painel de Preços (https://paineldeprecos.planejamento.gov.br/). Esta plataforma reúne registros de compras públicas homologadas no sistema de Compras do Governo Federal – COMPRASNET. O objetivo da referida base é auxiliar os gestores públicos na tomada de decisões nos processos de compra, garantir transparência nos preços praticados pela Administração Pública e estimular o controle social.

A equipe de planejamento da contratação buscou junto ao mercado, contratações, com as seguintes características: Escopo similar ao objeto, similaridades de requisitos negociais e tecnológicos, publicados recentemente e que foram atendidos com as soluções de mercado identificadas neste estudo técnico, e o resultado encontra-se abaixo:

Órgão	Unidade Compradora	Edital	Objeto
CONSELHO ADMINISTRATIVO DE DEFESA ECONOMICA-CADE	303001-CONSELHO ADMINISTRATIVO DE DEFESA ECONOMICA	90007/2024	Aquisição de equipamentos de proteção de rede, denominados Firewalls de Próxima Geração (Next Generation Firewall - NGFW) com proteção DNS, abrangendo serviços de planejamento, implementação e execução da migração entre equipamentos, solução de gerência centralizada e solução de armazenamento de logs com garantia e suporte técnico por 60 (sessenta) meses e fornecimento de toda documentação técnica gerada durante o período de implantação da solução e contra
DEPARTAMENTO DE TRÂNSITO DO DISTRITO FEDERAL	926142 - DEPARTAMENTO DE TRÂNSITO DO DISTRITO FEDERAL	90004/2024	Registro de Preço de solução de proteção de rede com características de Next Generation Firewall (NGFW) para segurança de informação perimetral
FUNDACAO NACIONAL DE ARTES FUNARTE	403201 - FUNDACAO NACIONAL DE ARTES	00004/2023	Registro de Preços para eventual contratação de solução de tecnologia da informação e comunicação de equipamento de segurança de rede, licenciamento de Firewall e direito de uso de appliance de Gerência Centralizada de NGFW com Gerenciador de Logs e Eventos, visando atender as necessidades da Fundação Nacional de Artes – FUNARTE.
		90009/2024	Solução de proteção de rede "Next Generation Firewall", contemplando os hardwares ,licenciamento, instalação, configuração, solução de armazenamento de logs e relatoria, Solução para gerenciamento centralizado dos equipamentos, treinamento, ZTNA, garantia e suporte técnico por 60 meses, de acordo com as condições, exigências,

MINISTERIO DA AGRICULTURA, PECUARIA E ABASTECIMENTO	130005 - COORD.-GERAL DE EXECUCAO ORç.E FIN./DA/MAPA		especificações e quantidades constantes deste termo de referência e seus Anexos.
MINISTERIO DA CULTURA	420001 - COORD. GERAL DE EXEC. ORCAMENT, FINANC E CONT	00009 /2023	Aquisição de uma solução de proteção de rede Next Generation Firewall (NGFW) com garantia e suporte, conforme condições e exigências estabelecidas no Termo de Referência 2/2023
PRESIDENCIA DA REPUBLICA	110001 - SECRETARIA DE ADMINISTRAÇÃO	00067 /2023	Aquisição de solução de equipamentos Firewall
PROCURADORIA GERAL DA JUSTICA	10640 - DEPTO MIN D E INFRAESTRUTURA DE TIC	116 /2023	Registro de Preços para Solução de FireWall Core e Solução De Autenticação De Usuários e Dispositivos (NAC)
PROCURADORIA GERAL DO ESTADO DO AMAPA	1 1 - PROCURADORIA-GERAL DO ESTADO	0190 /2023	AQUISIÇÃO DE SOLUÇÃO INTEGRADA DE FIREWALL COMPOSTA DE HARDWARE E SOFTWARE DE SEGURANÇA DA INFORMAÇÃO (PRODAP)
SANTA CATARINA TRIBUNAL DE JUSTICA	925045 - TRIBUNAL DE JUSTIÇA DO EST. DE SANTA CATARINA	00146 /2023	Contratação de serviço continuado de solução de Firewall, em regime de empreitada por preço global, conforme as especificações constantes do projeto básico.
SUPERIOR TRIBUNAL DE JUSTICA	050001 - STJ – SUPERIOR TRIBUNAL DE JUSTICA/DF	00110 /2023	Contratação de empresa especializada para fornecimento de solução de Web Application Firewall (WAF) com serviços de instalação, configuração, suporte técnico e treinamento
TRIBUNAL DE CONTAS DO DISTRITO FEDERAL	974003 - TRIBUNAL DE CONTAS DO DISTRITO FEDERAL	00018 /2023	Contratação de empresa especializada no fornecimento de soluções de segurança de redes de computadores, compostas de firewall corporativo e multifuncional, incluídos todos os softwares e suas licenças de uso por subscrição, gerenciamento centralizado, serviços de implantação, repasse de conhecimento da solução (treinamento), garantia de atualização contínua pelo período de 60 (sessenta) meses, a fim de atender às necessidades do TCDF.

b) **as alternativas do mercado** (IN/SGD/ME nº 94/2022 Art. 11, II, b)

O estudo técnico observou as soluções que se encontram no quadrante mágico do Gartner como "Leaders", foram identificados os seguintes fabricantes de solução de firewalls disponíveis no mercado:

Portanto, ainda que existem diferenças tecnológicas e de especificação técnica entre os diversos players de mercado, identifica-se a existência de várias opções preliminarmente compatíveis com a presente demanda, sendo que os três líderes de mercado (CheckPoint, Fortinet e Palo Alto) já oferecem soluções capazes de atender aos requisitos preliminares das unidades requisitantes.

c) **a existência de softwares disponíveis conforme descrito na Portaria STI/MP nº 46, de 28 de setembro de 2016, e suas atualizações** (IN/SGD/ME nº 94/2022 Art. 11, II, c e d)

Não foi encontrado em pesquisa software público que pudesse atender a demanda em análise de forma completa, uma vez que se trata da necessidade de um conjunto agregado de solução, além da oferta específica de equipamento especializado.

Registra-se também que, para essa solução nenhum dos padrões de governo, como e-Ping e demais, se aplicam.

e) **as necessidades de adequação do ambiente do órgão ou entidade para viabilizar a execução contratual** (IN/SGD/ME nº 94/2022 Art. 11, II, e)

Não há necessidade de adequação específica no ambiente físico para implantação da solução, tendo em vista que o tipo de solução já é muito utilizado pela maioria dos órgãos e entidades públicas, incluindo os órgãos requisitantes presentes, havendo apenas necessidade de substituição por solução atualizada e coberta por garantia do fabricante.

f) **os diferentes modelos de prestação do serviço** (IN/SGD/ME nº 94/2022 Art. 11, II, f)

O modelo de aquisição proposto exige a presença, no mínimo, dos seguintes principais atores:

1. **Fabricante da solução**: responsável por fornecer os equipamentos e softwares operacionais necessários, garantir o funcionamento dos produtos e, se necessário, oferecer treinamento na solução.

2. **Fornecedor**: atuando como intermediário, este profissional é encarregado de fornecer suporte técnico e intermediar ações junto ao fabricante. Neste caso, trata-se da Contratada.

3. **Consumidor da solução ou Cliente final**: representado pela Administração, que atua como Contratante.

Esses atores são essenciais em qualquer modelo de contratação. No entanto, o modelo em questão se fundamenta na aquisição e entrega de uma solução específica, acompanhada de suporte pós-venda.

g) **os diferentes tipos de soluções em termos de especificação, composição ou características dos bens e serviços integrantes** (IN/SGD/ME nº 94/2022 Art. 11, II, g)

Considerando a necessidade de negócio, os benefícios para Administração e as tecnologias disponíveis, foram prospectadas os seguintes cenários e soluções:

Solução 1 - Renovação do contrato atual

A solução atualmente utilizada pelo MCID está atrelada a dois entes públicos federais, que possuem gestões, contratos e equipes independentes. Assim, a renovação do contrato atual não se aplica, uma vez que esses contratos não são geridos pelo MCID. Além disso, a solução vigente deve proteger contra ameaças avançadas e persistentes que empregam técnicas de modificação de código, como polimorfismo e criptografia, que não são detectadas por sistemas tradicionais baseados em assinaturas.

Desvantagens:

- Falta de controle sobre a gestão e suporte.
- Dependência de políticas e contratos de terceiros.

Solução 2 – Utilização de software livre

Outra alternativa considerada é a adoção de software livre, como o PFSense, uma distribuição open source do FreeBSD.

Vantagens:

- Redução de custos com licenciamento de software.

Desvantagens:

- Ausência de suporte técnico 24x7, o que pode levar a riscos em situações críticas.
- Falta de funcionalidades de segurança avançada que são padrão em soluções proprietárias.
- Necessidade de treinamento para os usuários, impactando a curva de aprendizado e a produtividade.
- Incompatibilidade com ferramentas e formatos existentes, resultando em retrabalho e dificuldades de integração.

Solução 3 – Contratação de soluções de proteção avançada de perímetro

A aquisição de uma suíte de segurança para proteção avançada de perímetro é a solução mais alinhada com as práticas atuais para organizações de médio e grande porte. Essa abordagem oferece diversas vantagens, incluindo:

- **Detecção de Ameaças Avançadas:** Capacidade de identificar e responder a ameaças de dia zero.
- **Inspeção de Tráfego Criptografado:** Garantia de que o tráfego SSL/TLS não comprometa a segurança.
- **Filtragem de URL, Antimalware e Anti-Phishing:** Proteção contra uma ampla gama de ameaças.
- **Políticas de Segurança Granulares:** Permitem um controle mais preciso e eficiente.
- **Gerenciamento Centralizado:** Facilita a administração e a configuração da segurança da rede.

Comparação entre UTM e NGFW:

- O **Firewall UTM (Unified Threat Manager)** integra várias funcionalidades de segurança em uma única solução, como prevenção de intrusões, antivírus e filtragem de URL. É uma abordagem focada na simplicidade e facilidade de uso.

- O **Next Generation Firewall (NGFW)**, por outro lado, oferece uma inspeção de pacotes mais aprofundada e controle de acesso robusto, além de melhor detecção de atividades suspeitas e resposta mais ágil a ataques. Ele permite a implementação de políticas de controle mais eficazes para os desafios atuais da segurança digital.

Da comparação dos cenários:

REQUISITOS		**Há compatibilidade técnica da solução para atender a demanda? (SIM / NÃO)**		
		SOLUÇÃO 1	**SOLUÇÃO 2**	**SOLUÇÃO 3**
NEGÓCIO	Proteção de Dados Sensíveis	Não viável (Uma vez que o ministério não dispõe de infraestrutura própria).	X	X
	Conformidade com Normas e Regulamentações	Não viável (Uma vez que o ministério não dispõe de infraestrutura própria).		X
	Gerenciamento Eficiente de Recursos de TI	Não viável (Uma vez que o ministério não dispõe de infraestrutura própria).		X
	Aumento da Resiliência Cibernética	Não viável (Uma vez que o ministério não dispõe de infraestrutura própria).	X	X
	Apoio à Inovação e Modernização	Não viável (Uma vez que o ministério não dispõe de infraestrutura própria).		X
	Melhoria na Experiência do Usuário	Não viável (Uma vez que o ministério não dispõe de infraestrutura própria).		X
TECNOLÓGICO	Proteção Avançada e Multifuncional	Não viável (Uma vez que o ministério não dispõe de infraestrutura própria).		X
	Visibilidade Total do Tráfego de Rede	Não viável (Uma vez que o ministério não dispõe de infraestrutura própria).	X	X
	Gerenciamento Centralizado e Simplificado	Não viável (Uma vez que o ministério não dispõe de infraestrutura própria).	X	X
	Integração com Soluções Existentes	Não viável (Uma vez que o ministério não dispõe de infraestrutura própria).		X
	Capacidades de Resposta a Incidentes	Não viável (Uma vez que o ministério não dispõe de infraestrutura própria).	X	X
	Escalabilidade e Flexibilidade	Não viável (Uma vez que o ministério não dispõe de infraestrutura própria).		X

	Atualizações e Manutenção Contínuas	Não viável (Uma vez que o ministério não dispõe de infraestrutura própria).		X
Resultado da Análise		NÃO VIÁVEL	N Ã O VIÁVEL	**VIÁVEL**

Diante das análises, o **Solução 3** — a contratação de soluções de proteção avançada de perímetro — se destaca como a opção mais adequada para atender às necessidades de segurança do MCID. Com recursos avançados para prevenção de ameaças e uma abordagem moderna e integrada, essa solução não apenas fortalece a segurança da rede, mas também garante eficiência e agilidade na resposta a incidentes cibernéticos.

10. Registro de soluções consideradas inviáveis

Durante o processo de análise para a proteção avançada de perímetro no Ministério das Cidades (MCID), algumas soluções foram consideradas inviáveis devido a limitações significativas que comprometem sua eficácia e adequação às necessidades específicas do órgão. Abaixo, estão detalhadas as opções descartadas e as razões para tal decisão.

Solução 1 - Renovação do Contrato Atual

Descrição: A solução atualmente em uso pelo MCID está vinculada a contratos com dois entes públicos federais, cada um com sua gestão, políticas e equipes independentes.

Motivos da inviabilidade:

- **Dependência Externa:** A renovação implicaria em continuar a dependência de órgãos externos, o que limita a autonomia do MCID na implementação de medidas de segurança adaptadas às suas necessidades específicas.
- **Gestão Fragmentada:** Com equipes distintas gerenciando as soluções, a coordenação de incidentes e a resposta a ameaças se tornam ineficazes, aumentando o tempo de resolução e expondo a organização a riscos maiores.
- **Incompatibilidade Técnica:** A divergência entre as tecnologias e práticas de segurança utilizadas pelos entes parceiros e as necessidades do MCID pode comprometer a eficácia da proteção contra novas ameaças. Essa incompatibilidade dificulta a integração de sistemas e a implementação de uma estratégia de segurança unificada.

Solução 2 - Utilização de Software Livre

Descrição: A consideração de uma solução de código aberto, como o PFSense, que oferece funcionalidades básicas de firewall e segurança.

Motivos da inviabilidade:

- **Falta de Suporte Técnico:** A ausência de suporte 24x7 representa um risco significativo, especialmente em um cenário de ataque cibernético, onde a prontidão para responder a incidentes é crucial.
- **Recursos Limitados:** O PFSense não oferece as funcionalidades avançadas de segurança que as soluções comerciais garantem, como detecção de ameaças de dia zero, inspeção SSL e recursos de inteligência cibernética.
- **Treinamento e Adaptação:** A necessidade de treinar a equipe em uma nova plataforma pode levar a perdas de produtividade e tempo, além de dificultar a adaptação devido à familiaridade com soluções já existentes.
- **Incompatibilidade com o Ecossistema:** A mudança para uma solução open source pode gerar problemas de compatibilidade com sistemas e formatos já utilizados, resultando em retrabalho e resistência por parte dos usuários.

As soluções consideradas inviáveis demonstraram limitações significativas em relação à autonomia, eficiência e eficácia necessárias para a segurança do MCID. Assim, o foco deve ser em opções que proporcionem uma abordagem integrada e robusta, capaz de atender às demandas atuais e futuras de segurança cibernética.

11. Análise comparativa de custos (TCO)

Composição da solução

A análise comparativa de custos foi elaborada considerando apenas as soluções técnica e funcionalmente viáveis, nos termos do inc. III art. 11 da IN-94/2022/SGD, e inclui:

comparação de custos totais de propriedade (Total Cost Ownership – TCO) por meio da obtenção dos custos inerentes ao ciclo de vida dos bens e serviços de cada solução, a exemplo dos valores de aquisição dos ativos, insumos, garantia, manutenção; e

memória de cálculo que referencie os preços e os custos utilizados na análise, com vistas a permitir a verificação da origem dos dados.

CÁLCULO DOS CUSTOS TOTAIS DE PROPRIEDADE (TCO)

Conforme determinado na Instrução Normativa SGD/ME nº 94, de 23 de dezembro de 2022, deverá ser realizada a análise comparativa de custos envolvidos na contratação. Para isso, deverão ser consideradas somente as soluções **viáveis**, bastando o registro das soluções inviáveis no Estudo Técnico Preliminar da Contratação:

Art. 11

(...)

III - análise comparativa de custos, que deverá considerar apenas as soluções técnica e funcionalmente viáveis, incluindo:

a) cálculo dos custos totais de propriedade (**Total Cost Ownership** - TCO) por meio da obtenção dos custos inerentes ao ciclo de vida dos bens e serviços de cada solução, a exemplo dos valores de aquisição dos ativos, insumos, garantia técnica estendida, manutenção, migração e treinamento; e

b) memória de cálculo que referencie os preços e os custos utilizados na análise, com vistas a permitir a verificação da origem dos dados;

IV - estimativa do custo total da contratação; e

V - declaração da viabilidade da contratação, contendo a justificativa da solução escolhida, que deverá abranger a identificação dos benefícios a serem alcançados em termos de eficácia, eficiência, efetividade e economicidade.

§ 1º As soluções identificadas no inciso II consideradas inviáveis deverão ser registradas no Estudo Técnico Preliminar da Contratação, dispensando-se a realização dos respectivos cálculos de custo total de propriedade.

Conforme discutido nos tópicos anteriores deste ETP, a **Solução 3 – Contratação de soluções de proteção avançada de perímetro** foi identificada como a melhor alternativa entre as opções avaliadas. Essa aquisição será realizada por meio de recursos orçamentários de investimento do Ministério das Cidades.

Após a definição da composição da solução de tecnologia da informação a ser adquirida, conforme registrado no item 9 deste estudo, verifica-se a necessidade da realização dos procedimentos para a estimativa de custos para a aquisição da solução.

Neste sentido, verifica-se que o levantamento dos valores para a aquisição de bens e contratação de serviços em geral para os órgãos e entidades participantes do SISG - Sistema de Serviços Gerais, deve seguir os procedimentos administrativos definidos pela INSTRUÇÃO NORMATIVA SEGES /ME Nº 65, DE 7 DE JULHO DE 2021 da Secretaria de Gestão (SEGES) do Ministério da Economia. Para tanto, este levantamento servirá para balizar a viabilidade financeira do projeto.

Em atendimento ao art. 5º da Instrução Normativa nº 65, de 07 de Julho de 2021:

Art. 5º A pesquisa de preços para fins de determinação do preço estimado em processo licitatório para a aquisição de bens e contratação de serviços em geral será realizada mediante a utilização dos seguintes parâmetros, empregados de forma combinada ou não:
I - composição de custos unitários menores ou iguais à mediana do item correspondente nos sistemas oficiais de governo, como Painel de Preços ou banco de preços em saúde, observado o índice de atualização de preços correspondente;
II - contratações similares feitas pela Administração Pública, em execução ou concluídas no período de 1 (um) ano anterior à data da pesquisa de preços, inclusive mediante sistema de registro de preços, observado o índice de atualização de preços correspondente;
III - dados de pesquisa publicada em mídia especializada, de tabela de referência formalmente aprovada pelo Poder Executivo federal e de sítios eletrônicos especializados ou de domínio amplo, desde que atualizados no momento da pesquisa e

compreendidos no intervalo de até 6 (seis) meses de antecedência da data de divulgação do edital, contendo a data e a hora de acesso;
IV - pesquisa direta com, no mínimo, 3 (três) fornecedores, mediante solicitação formal de cotação, por meio de ofício ou e-mail, desde que seja apresentada justificativa da escolha desses fornecedores e que não tenham sido obtidos os orçamentos com mais de 6 (seis) meses de antecedência da data de divulgação do edital; ou
V - pesquisa na base nacional de notas fiscais eletrônicas, desde que a data das notas fiscais esteja compreendida no período de até 1 (um) ano anterior à data de divulgação do edital, conforme disposto no Caderno de Logística, elaborado pela Secretaria de Gestão da Secretaria Especial de Desburocratização, Gestão e Governo Digital do Ministério da Economia.
§ 1º Deverão ser priorizados os parâmetros estabelecidos nos incisos I e II, devendo, em caso de impossibilidade, apresentar justificativa nos autos.
§ 2º Quando a pesquisa de preços for realizada com fornecedores, nos termos do inciso IV, deverá ser observado:
I - prazo de resposta conferido ao fornecedor compatível com a complexidade do objeto a ser licitado;
II - obtenção de propostas formais, contendo, no mínimo:
a) descrição do objeto, valor unitário e total;
b) número do Cadastro de Pessoa Física - CPF ou do Cadastro Nacional de Pessoa Jurídica - CNPJ do proponente;
c) endereços físico e eletrônico e telefone de contato;
d) data de emissão; e
e) nome completo e identificação do responsável.
III - informação aos fornecedores das características da contratação contidas no art. 4º, com vistas à melhor caracterização das condições comerciais praticadas para o objeto a ser contratado; e
IV - registro, nos autos do processo da contratação correspondente, da relação de fornecedores que foram consultados e não enviaram propostas como resposta à solicitação, de que trata o inciso IV do caput.
§ 3º Excepcionalmente, será admitido o preço estimado com base em orçamento fora do prazo estipulado no inciso II do caput, desde que devidamente justificado nos autos pelo agente responsável e observado o índice de atualização de preços correspondente.

O custo estimado para a contratação em questão foi calculado, tendo como base o valor unitário extraído da Pesquisa de Preços (SEI nº 5431341).

ITEM	**DESCRIÇÃO**	**UNIDADE D E MEDIDA**	**QUANTIDADE**	**VALOR UNITÁRIO**	**TOTAL**
1	Solução de segurança em Cluster para proteção avançada de perímetro - Firewall - denominada Next Generation Firewall (NGFW) com suporte, garantia e licenciamento inclusos para 60 meses com repasse de conhecimento.	Unidade	4	R $ 1.896.136,16	R $ 7.584.544,6
2	Solução para Gerenciamento de LOGS e Automação	Unidade	1	R $ 137.419,70	R $ 137.419,70
3	Solução para Gerenciamento Centralizado de NGFW	Unidade	1	R $ 88.123,00	R $ 88.123,00
4	Instalação e Configuração	Unidade	1	R $ 67.514,24	R $ 67.514,24
VALOR GLOBAL ESTIMADO				**R$ 7.877.601,58**	

12. Descrição da solução de TIC a ser contratada

A segurança da rede é um componente crítico para a proteção das informações e ativos de qualquer organização, e os firewalls desempenham um papel fundamental nesse contexto. Desde sua introdução na década de 1980, essas soluções têm evoluído, mas, como evidenciado por este estudo, um firewall isolado não é suficiente para garantir a segurança total de uma rede ou computador. Portanto, é essencial integrá-lo a outros recursos de segurança, como antivírus, sistemas de detecção de intrusos, filtros de conteúdo web e VPN (Virtual Private Network), formando uma abordagem multifuncional e robusta.

Um firewall, seja em hardware ou software, opera com base em um conjunto de regras que analisa o tráfego de rede, determinando quais operações de transmissão ou recepção de dados são permitidas. A utilização de um firewall de hardware traz vantagens significativas, uma vez que este equipamento é projetado especificamente para lidar com grandes volumes de dados e não está exposto às vulnerabilidades comuns de servidores convencionais, que podem ocorrer devido a falhas em outros softwares.

Objetivo da Solução

A solução proposta visa a aquisição de firewalls corporativos multifuncionais que garantirão a segurança da rede de computadores do Ministério das Cidades (MCID). Esta solução deve oferecer uma gerência unificada, assegurando a continuidade do funcionamento por um período de 60 (sessenta) meses. O pacote de aquisição incluirá todos os softwares necessários, suas licenças de uso, gerenciamento centralizado, serviços de implantação e garantia de atualização contínua. Além disso, será disponibilizado suporte técnico durante todo o período de garantia, com repasse de conhecimento sobre a solução.

Composição da Solução

A solução a ser contratada terá como composição:

ITEM	DESCRIÇÃO	SUB-DESCRIÇÃO	UNIDADE DE MEDIDA	QUANTIDADE
1	Solução de segurança em Cluster para proteção avançada de perímetro - Firewall - denominada Next Generation Firewall(NGFW) com suporte, garantia e licenciamento inclusos para 60 meses com repasse de conhecimento.	Hardware /Licenciamento	Unidade	4
2	Solução para Gerenciamento de LOGS e Automação		Unidade	1
3	Solução para Gerenciamento Centralizado de NGFW		Unidade	1
4	Instalação e Configuração		Unidade	1

A solução proposta, com dois clusters de firewall, cada um com duas unidades, garante a alta disponibilidade e a escalabilidade necessárias para atender às demandas do Ministério das Cidades. Essa arquitetura redundante distribui a carga de trabalho, otimiza o desempenho e minimiza o risco de interrupções no serviço. Além disso, a solução oferece a flexibilidade necessária para acompanhar o crescimento da rede e as mudanças no cenário de ameaças, proporcionando uma proteção robusta e adaptável aos desafios da segurança cibernética.

O prazo de vigência da contratação será de 60 (sessenta) meses contados da assinatura do contrato, na forma do artigo 105 da Lei n° 14.133, de 2021.

O objeto da contratação NÃO incide nas hipóteses vedadas pelos artigos 3º, 4º e 5º da IN SGD nº 94/2022:

Art. 3º Não poderão ser objeto de contratação:

I - mais de uma solução de TIC em um único contrato, devendo o órgão ou entidade observar o disposto nos §§ 2º e 3º do art. 12; e

II - os serviços dispostos no art. 3º do Decreto nº 9.507, de 2018, inclusive a gestão de processos de TIC e a gestão de segurança da informação.

Parágrafo único. O apoio técnico aos processos de gestão, de planejamento e de avaliação da qualidade das soluções de TIC poderá ser objeto de contratação, desde que sob supervisão exclusiva de servidores do órgão ou entidade.

Art. 4º Nos casos em que a avaliação, mensuração ou apoio à fiscalização da solução de TIC seja objeto de contratação, a contratada que provê a solução de TIC não poderá ser a mesma que a avalia, mensura ou apoia a fiscalização.

Parágrafo único. A empresa ou o profissional contratado assumirá responsabilidade civil objetiva pela veracidade e pela precisão das informações prestadas, firmará termo de compromisso de confidencialidade e não poderá exercer atribuição própria e exclusiva de fiscal de contrato, conforme dispõe o art. 26, do Decreto nº 11.246, de 27 de outubro de 2022.

Art. 5º É vedado:

I - estabelecer vínculo de subordinação com funcionário de empresa prestadora de serviço terceirizado;

II - fixar salário inferior ao definido em lei ou em ato normativo a ser pago pelo contratado;

III - indicar pessoas expressamente nominadas para executar direta ou indiretamente o objeto contratado;

IV - demandar a funcionário de empresa prestadora de serviço terceirizado a execução de tarefas fora do escopo do objeto da contratação;

V - reembolsar despesas com transporte, hospedagem e outros custos operacionais, que devem ser de exclusiva responsabilidade da contratada;

VI - prever em edital exigências que constituam intervenção indevida da Administração na gestão interna do contratado;

VII - prever em edital exigência que os fornecedores apresentem, em seus quadros, funcionários capacitados ou certificados para o fornecimento da solução, antes da contratação;

VIII - adotar a métrica homem-hora ou equivalente para aferição de esforço, salvo mediante justificativa e sempre vinculada à entrega de produtos de acordo com prazos e qualidade previamente definidos;

IX - contratar por postos de trabalho alocados, salvo os casos justificados mediante a comprovação obrigatória de resultados compatíveis com o posto previamente definido;

X - fazer referências, em edital ou em contrato, a regras externas de fabricantes, fornecedores ou prestadores de serviços que possam acarretar na alteração unilateral do contrato por parte da contratada;

XI - nas licitações do tipo técnica e preço, incluir critérios de pontuação técnica que não estejam diretamente relacionados com os requisitos da solução de TIC a ser contratada ou que frustrem o caráter competitivo do certame;

XII - aceitar autodeclarações de exclusividade, ou seja, cartas ou declarações emitidas pela empresa proponente afirmando que seu próprio produto é exclusivo no mercado; e

XIII - definir forma de pagamento mediante exclusivo reembolso dos salários pagos.

13. Estimativa de custo total da contratação

Valor (R$): 7.877.601,58

A estimativa de custo total para a presente aquisição, de acordo com as necessidades do Ministério das Cidades, é de **R$ 7.877.601,58 (sete milhões, oitocentos e setenta e sete mil seiscentos e um reais e cinquenta e oito centavos)** conforme tabela detalhada abaixo:

ITEM	DESCRIÇÃO	UNIDADE D E MEDIDA	QUANTIDADE	VALOR UNITÁRIO	TOTAL

1	Solução de segurança em Cluster para proteção avançada de perímetro - Firewall - denominada Next Generation Firewall (NGFW) com suporte, garantia e licenciamento inclusos para 60 meses com repasse de conhecimento.	Unidade	4	R $ 1.896.136,16	R $ 7.584.544,64
2	Solução para Gerenciamento de LOGS e Automação	Unidade	1	R $ 137.419,70	R $ 137.419,70
3	Solução para Gerenciamento Centralizado de NGFW	Unidade	1	R $ 88.123,00	R $ 88.123,00
4	Instalação e Configuração	Unidade	1	R $ 67.514,24	R $ 67.514,24
VALOR GLOBAL ESTIMADO				**R$ 7.877.601,58**	

14. Justificativa técnica da escolha da solução

Após uma análise detalhada das opções disponíveis, a melhor e mais viável solução para o Ministério das Cidades (MCID) é a **Contratação de Soluções Avançadas de Proteção de Perímetro**, conforme identificado no Cenário 3. Esta escolha é fundamentada em diversas considerações técnicas que se alinham às necessidades e requisitos do departamento de segurança da informação, especialmente diante da descontinuidade da centralização da gestão da segurança cibernética pela FUNASA, prevista para janeiro de 2025.

Benefícios Técnicos da Solução Avançada

1. **Nível Superior de Segurança:** A adoção de uma solução avançada de proteção de perímetro proporciona um nível de segurança significativamente maior, capaz de enfrentar as ameaças cibernéticas mais sofisticadas, como malwares avançados, ataques DDoS e intrusões persistentes.

2. **Capacidade de Processamento Aumentada:** Com uma infraestrutura projetada para suportar altos volumes de tráfego, a solução permitirá a implementação de novos serviços, como análise de tráfego e gestão centralizada de logs. Isso facilita a automação dos fluxos de resposta a incidentes, otimizando a eficiência operacional da equipe de segurança.

3. **Visibilidade Detalhada:** A solução oferece uma visualização abrangente do uso da rede e das aplicações em funcionamento, permitindo a identificação de padrões e comportamentos que possam indicar atividades suspeitas. Essa transparência é crucial para a aplicação de políticas de segurança mais eficazes e direcionadas.

Justificativa para a Arquitetura em Cluster

A escolha de implementar uma arquitetura em cluster é igualmente estratégica. As principais justificativas incluem:

- **Alta Disponibilidade:** A configuração em cluster garante a redundância e a continuidade dos serviços, minimizando o risco de interrupções em caso de falhas em um dos dispositivos. Isso é essencial para manter a integridade e a disponibilidade da rede, especialmente em ambientes críticos.

- **Escalabilidade:** A arquitetura em cluster permite uma fácil expansão da capacidade de processamento conforme a demanda aumenta, possibilitando que o MCID se adapte rapidamente às necessidades futuras sem comprometer a segurança.

- **Distribuição de Carga:** A distribuição da carga de trabalho entre os equipamentos do cluster não apenas otimiza o desempenho, mas também assegura que o tráfego seja gerenciado de forma eficiente, reduzindo latências e melhorando a experiência do usuário.

Dessa forma, a escolha de uma solução avançada de proteção de perímetro, com arquitetura em cluster, não é apenas a mais adequada do ponto de vista técnico, mas também alinhada às diretrizes de segurança do MCID. Esta abordagem assegurará a proteção robusta necessária para enfrentar os desafios da cibersegurança contemporânea, garantindo a continuidade das operações e a proteção dos dados sensíveis da instituição.

15. Justificativa econômica da escolha da solução

A escolha da solução de proteção avançada de perímetro para o Ministério das Cidades (MCID) foi fundamentada não apenas em aspectos técnicos, mas também em uma análise detalhada dos benefícios econômicos que esta solução proporciona em comparação com as alternativas consideradas. A seguir, destacamos os principais pontos que sustentam essa justificativa econômica:

1. **Análise do Custo Total de Propriedade (TCO)**

O Custo Total de Propriedade (TCO) é um fator crítico na avaliação das soluções de segurança. Ao considerar o TCO, observamos que a solução de proteção avançada de perímetro, apesar de apresentar um custo inicial elevado, oferece uma série de vantagens econômicas a longo prazo, que incluem:

- **Redução de Custos com Manutenção e Suporte:** A solução escolhida oferece suporte técnico contínuo e atualizações regulares, minimizando custos inesperados de manutenção e garantindo que a segurança da rede esteja sempre atualizada. Comparado às soluções de software livre, que podem acarretar gastos significativos com suporte técnico não garantido, a escolha se mostra mais econômica.

- **Eficiência Operacional:** A automação de processos e a gestão centralizada da nova solução reduzirão o tempo e os recursos necessários para monitorar e gerenciar a segurança da rede, resultando em economias significativas em mão de obra e esforço administrativo.

2. **Vantagens do Sistema de Registro de Preços**

Optar pela contratação através do Sistema de Registro de Preços proporciona uma série de vantagens econômicas:

- **Estabilidade de Preços:** A possibilidade de registrar preços fixos para os itens contratados evita oscilações no custo ao longo do tempo, protegendo o MCID de aumentos inesperados nos preços dos produtos e serviços necessários para a implementação e manutenção da solução.

- **Entregas Parceladas:** O sistema de entregas parceladas possibilita um melhor planejamento financeiro, permitindo que o MCID dilua os custos ao longo do período de contrato. Isso garante uma melhor alocação de recursos, evitando a pressão sobre o orçamento em momentos críticos.

3. **Economias de Escala e Ganhos Processuais em Compras Conjuntas**

Embora a solução escolhida não envolva compras conjuntas diretamente, o conceito de economias de escala ainda se aplica:

- **Aumento da Capacidade de Negociação:** Ao contratar uma solução mais robusta, o MCID está em posição de negociar termos mais favoráveis com fornecedores, aproveitando a possibilidade de aquisições em larga escala.

- **Redução do Esforço de Gestão:** A centralização e unificação da gestão de segurança, possibilitadas pela nova solução, diminuem a complexidade do processo de contratação e gerenciamento, resultando em economia de tempo e recursos na execução de atividades administrativas.

4. **Proteção Contra Custos Ocultos de Segurança**

Investir em uma solução avançada de segurança é uma medida preventiva que pode evitar custos significativos decorrentes de incidentes de segurança, como vazamentos de dados e interrupções operacionais. Esses eventos podem resultar em:

- **Multas e Penalidades:** A não conformidade com regulamentações de segurança pode gerar penalidades financeiras substanciais.

- **Perda de Reputação:** Incidentes de segurança podem afetar a confiança do público e dos parceiros, resultando em perdas econômicas que vão além dos custos diretos.

Diante dos fatores econômicos apresentados, a escolha da solução de proteção avançada de perímetro se justifica plenamente. A análise do TCO demonstra que, embora o investimento inicial seja considerável, os benefícios a longo prazo, a estabilidade de preços, a eficiência operacional e a mitigação de riscos financeiros associam-se a uma escolha que proporciona segurança e viabilidade econômica ao MCID. Assim, esta solução não apenas atende às necessidades de segurança da informação, mas também se apresenta como uma opção economicamente vantajosa para a instituição.

16. DO PARCELAMENTO DA CONTRATAÇÃO

DO PARCELAMENTO DA CONTRATAÇÃO DECORRENTE DE ASPECTOS TÉCNICOS

A proposta de parcelamento da contratação da solução de segurança de perímetro é fundamentada em uma série de fatores técnicos que garantem a eficácia da implementação e a adequada integração dos novos sistemas na infraestrutura existente do Ministério das Cidades (MCID). A seguir, detalhamos as principais razões para essa abordagem:

1. **Fatores Logísticos e de Armazenagem**

A contratação de uma solução complexa como a de segurança de perímetro envolve a aquisição de múltiplos componentes, incluindo hardware e software, que podem demandar um espaço físico considerável. O parcelamento permitirá que o MCID gerencie a logística de recebimento e armazenagem dos itens de forma mais eficiente, evitando sobrecarga nas instalações e garantindo que cada componente seja devidamente integrado antes da chegada do próximo.

2. **Desenvolvimento Modular e Dependência de Componentes**

A solução proposta será composta por diferentes módulos que podem depender uns dos outros para operar de maneira eficaz. O parcelamento possibilita a implementação em etapas, permitindo que cada módulo seja testado e otimizado antes da introdução do próximo. Isso não apenas minimiza riscos técnicos, mas também assegura que o sistema final funcione de maneira coesa e integrada.

3. **Preparação da Estrutura Física**

A adoção de uma nova infraestrutura de TI pode exigir adaptações nas instalações físicas, como adequações elétricas, climatização e espaço físico para os novos equipamentos. O parcelamento oferece a flexibilidade necessária para preparar essa infraestrutura de maneira adequada, garantindo que todas as condições estejam atendidas antes da instalação dos novos sistemas. Essa preparação é crucial para maximizar a vida útil dos equipamentos e assegurar o seu funcionamento ideal.

4. **Treinamento e Capacitação da Equipe**

Com a introdução de novas tecnologias, o MCID necessitará de um período adequado para treinamento e capacitação da equipe técnica. O parcelamento permitirá que o treinamento seja realizado de forma escalonada, alinhando a formação dos profissionais com a entrega e implementação dos módulos, garantindo que a equipe esteja plenamente preparada para operar e gerenciar as novas soluções.

5. **Gestão de Recursos Financeiros**

O parcelamento também se justifica do ponto de vista orçamentário, permitindo uma melhor gestão dos recursos financeiros disponíveis. Essa abordagem facilita o planejamento do fluxo de caixa e possibilita alocar os investimentos de maneira mais estratégica, garantindo que o MCID mantenha a saúde financeira enquanto realiza a implementação da nova solução.

Diante dos fatores técnicos apresentados, a adoção do parcelamento na contratação da solução de segurança de perímetro se revela não apenas prudente, mas essencial para garantir uma implementação bem-sucedida e integrada. Essa estratégia assegurará que todos os aspectos técnicos, logísticos e operacionais sejam cuidadosamente considerados, contribuindo para a eficácia e segurança da infraestrutura de TI do MCID.

DO PARCELAMENTO DA CONTRATAÇÃO

Sob a ótica negocial, a correlação, a interdependência para adequada execução dos serviços e a unicidade dos serviços contratados inviabilizam o parcelamento dos itens em lotes distintos, que por sua vez, acarretaria, além de um custo maior para

Administração, risco de execução iminente e, adicionalmente, afetaria negativamente a imagem da prestação do serviço público ao cidadão proposto.

Sob uma perspectiva técnica, a escolha de um único fornecedor para a solução de proteção avançada de perímetro oferece uma série de vantagens significativas. A integração de diversos componentes e funcionalidades ofertados por um único fornecedor proporciona maior compatibilidade e interoperabilidade entre os elementos, evitando conflitos e incompatibilidades técnicas que poderiam surgir ao lidar com múltiplos fornecedores.

Outra vantagem técnica é a facilidade no suporte e resolução de problemas. Ao ter um único ponto de contato para o suporte técnico, as questões podem ser tratadas de forma mais eficiente e coordenada, garantindo uma assistência rápida em caso de necessidade. A complexidade de lidar com múltiplos fornecedores e suas respectivas equipes de suporte é minimizada.

Uma solução integrada e consolidada oferece a oportunidade de implementar melhores práticas de segurança de forma mais abrangente e consistente. Isso ocorre porque os diversos componentes são projetados para funcionar como um ecossistema, e um único fornecedor é componente chave para essa consistência e harmonia, permitindo a aplicação de políticas de segurança consistentes em todo o ambiente computacional.

Do ponto de vista da implementação, a execução de toda solução por um único fornecedor também pode resultar em redução de tempo e esforço. A integração e configuração entre os diferentes componentes são otimizadas, o que pode acelerar o processo de implantação. A manutenção continua também é simplificada, e o monitoramento com abordagem de inteligência cibernética adaptativa terá sua condução mais ágil e consistente, com a disponibilização de interface e lógica consistentes em todos os módulos. uma vez que as atualizações e melhorias são gerenciadas de maneira mais centralizada e com unicidade de processos.

A escolha de um único fornecedor deve ser baseada em critérios objetivos, como a eficácia da solução, a qualidade do suporte técnico, a integração dos componentes e a capacidade de atender aos requisitos específicos do órgão. Tais fundamentos técnicos sólidos apoiam a justificativa de optar por um único fornecedor para a solução de proteção avançada de perímetro.

Do ponto de vista administrativo, no Acórdão 5301/2013 – Segunda Câmara - TCU entendeu como legítima a reunião em grupo de elementos de mesma característica, quando a adjudicação por itens isolados onerar “o trabalho da administração pública, sob o ponto de vista do emprego de recursos humanos e da dificuldade de controle, colocando em risco a economia de escala e a celeridade processual”, o que pode comprometer a seleção da proposta mais vantajosa.

Baseado neste contexto é importante ressaltar que, no acórdão 5134/2014-TCU-Segunda Câmara, à tulo de exemplo, o Tribunal de Contas da União se manifestou no sentido de que a adjudicação por lote em detrimento da adjudicação por item não necessariamente implica restrição ao caráter competitivo do certame, devendo, inicialmente, ser analisado o caso concreto.

O Ministro José Jorge, relator do referido acórdão, consignou no seu voto:

“6. (...) a questão debatida se resume ao critério de julgamento adotado no Pregão Eletrônico 01/2014 ['registro de preços de equipamentos de uso e de proteção individual para servidores policiais que atuarão nas atividades de instrutor de tiro, operador de fuzil e grupo de pronta intervenção, para atender a demanda da Superintendência Regional - BA do Departamento de Polícia Federal e outras unidades'], qual seja, o de menor preço global, com a adjudicação por lote, em detrimento da adjudicação por item licitado.

7. A en dade sustenta que o critério por lote foi escolhido por duas razões: a uma, porque os itens agrupados possuem a mesma natureza, para uso específico em a vidade policial; e, a duas, porque a maioria dos licitantes fornece a totalidade dos itens especificados. Não haveria, portanto, restrição ao caráter compe vo do certame.

[...]

10. No caso em tela, algumas considerações devem ser feitas. No primeiro momento, observo que a jus fica va apresentada pela Polícia Federal, especificamente quanto à alegação de que os itens agrupados possuem a mesma natureza, me parece razoável.

[...]

21. Não vejo, portanto, a alegada afronta à jurisprudência do Tribunal. A interpretação da Súmula/TCU 247 não pode se restringir à sua literalidade, quando ela se refere a itens. A par r de uma interpretação sistêmica, há de se entender itens, lotes e grupos.

Objetos de mesma natureza constituem um "gênero", do qual são "espécies" os itens que se inserem em um mesmo ramo de atividade. É importante registrar que a adjudicação por item não acarretaria nenhum aumento na competição, haja vista que não existe um mercado específico para cada um desses itens.

Destacamos ainda a interdependência entre os itens, tornando inviável, do ponto de vista técnico, sua execução de forma separada, pois isso acarretaria grande prejuízo ao órgão e riscos técnicos e operacionais.

Nesse sentido, torna-se mais vantajoso para a Administração Pública a contratação de um fornecedor único para as atividades que envolvem a solução objeto desta contratação.

Assim, a divisão do objeto em lotes distintos não é adequada do ponto de vista técnico e de governança dos serviços prestados. Todos os serviços elencados têm correlação entre si, e a gestão do funcionamento e atendimento deve ser totalmente integrada, sob pena de comprometer a governança e a eficiência dos serviços contratados.

Adicionalmente, a contratação proposta não afasta os princípios da economicidade e da competitividade. Ao contrário, além de possibilitar a facilidade de repasse de conhecimentos da CONTRATADA para o Ministério das Cidades por meio de metodologias únicas, evita atrasos e retrabalhos oriundos de CONTRATADAS distintas. Embora a Súmula n° 247 do TCU determine que o parcelamento é a regra, essa diretriz se aplica apenas se for técnica e economicamente viável.

No caso, portanto, da "compra do item do mesmo fornecedor", ou seja, na situação em que os itens demandados pertencem a um mesmo ramo de atividade (hipótese em que os potenciais licitantes seriam os mesmos), o fato de não haver parcelamento não implicaria redução automática da competitividade, tampouco prejuízo econômico à Administração.

Além disso, a decisão de optar pelo parcelamento da solução de proteção avançada de perímetro para o Ministério das Cidades (MCID) é fundamentada em diversos fatores econômicos que garantem uma abordagem financeira mais sustentável e vantajosa. A seguir, apresentamos os principais pontos que justificam essa escolha:

1. **Disponibilidade Orçamentária**

O parcelamento da contratação permite uma melhor gestão do orçamento disponível, facilitando a alocação de recursos financeiros ao longo do tempo. Ao dividir o investimento em parcelas, o MCID pode:

- **Preservar Fluxo de Caixa:** O parcelamento evita um desembolso financeiro elevado em um único momento, permitindo que o órgão mantenha uma reserva de caixa para outras despesas operacionais e emergenciais que possam surgir ao longo do exercício.

- **Adequação ao Planejamento Orçamentário:** Com a possibilidade de parcelar o pagamento, o MCID pode planejar e ajustar seu orçamento de acordo com as disponibilidades anuais, minimizando o impacto financeiro e assegurando que outras áreas também sejam atendidas.

2. **Ganhos de Escala**

O parcelamento pode ser aliado a uma estratégia de aquisição que aproveite os ganhos de escala, resultando em:

- **Redução dos Valores Unitários:** Ao optar por um contrato parcelado, é possível negociar quantidades maiores ao longo do tempo, o que pode resultar em melhores condições de compra e descontos progressivos. Assim, o MCID pode se beneficiar de reduções significativas nos custos unitários à medida que a quantidade total adquirida aumenta.

- **Melhores Condições Comerciais:** Fornecedores costumam estar mais dispostos a oferecer preços mais competitivos e condições de pagamento favoráveis quando há a promessa de um volume maior de compras ao longo do tempo.

3. **Flexibilidade Financeira**

O parcelamento confere maior flexibilidade financeira ao MCID, permitindo que o órgão:

- **Adapte-se a Mudanças de Cenário:** Em um ambiente econômico dinâmico, o parcelamento oferece a capacidade de ajustar o planejamento financeiro conforme mudanças nas necessidades e prioridades da instituição.

- **Gerencie Riscos Financeiros:** A diluição do pagamento em parcelas reduz o risco de comprometer recursos significativos em um único investimento, garantindo que o MCID possa responder a eventuais imprevistos financeiros sem comprometer sua capacidade operacional.

Diante dos fatores econômicos apresentados, a justificativa para o parcelamento da solução de proteção avançada de perímetro se revela robusta. A combinação da disponibilidade orçamentária, os ganhos de escala na aquisição e a flexibilidade financeira proporcionada pelo parcelamento garantem que o MCID possa realizar um investimento seguro e sustentável, alinhado às suas necessidades operacionais e orçamentárias. Essa abordagem não apenas facilita a implementação da solução, mas também assegura a continuidade das atividades do ministério sem comprometer sua saúde financeira.

17. Benefícios a serem alcançados com a contratação

A declaração da viabilidade da contratação expressa nesta seção apresenta a justificativa da solução escolhida, abrangendo a identificação dos benefícios a serem alcançados em termos de eficácia, eficiência, efetividade e economicidade.

Nesse sentido, o planejamento em tela almejou os seguintes resultados:

Eficiência com a redução do custo administrativo e operacional em função do agrupamento de itens em uma solução de segurança cibernética consolidada e unificada;

Economia no valor da licitação em função do ganho de escala e na forma agrupada de contratação;

Efetividade com a padronização dos itens previstos, subscrições e aumento da qualidade das especificações técnicas;

Conformidade Legal: Adequação às legislações atuais, como a LGPD (Lei nº 13.709/2018) e o Marco Civil da Internet (Lei nº 12.965/2014).

Segurança da Informação: Manutenção dos requisitos de segurança, garantindo a integridade, confidencialidade e disponibilidade dos dados.

Visibilidade Aumentada: Melhoria na observação do uso de aplicações web e desktop, tráfego de rede e identificação de principais ameaças cibernéticas.

Detecção em Tempo Real: Capacidade de detectar e prevenir ameaças cibernéticas imediatamente.

Controle de Rede: Gestão do uso da rede, permitindo a aplicação de filtros e bloqueios de acordo com o perfil do usuário, controlando o acesso de maneira detalhada.

Proteção do Ambiente: Defesa contra ameaças como worms, vírus, malwares e APTs, em conformidade com o Marco Civil da Internet.

Geração de Relatórios: Produção de relatórios variados para uma análise rápida sobre tráfego, aplicações, ameaças e usuários.

Prevenção de Vazamento de Dados: Proteção contra exfiltração de dados, em linha com a LGPD.

Controle de Acesso Geográfico: Implementação de restrições de acesso baseadas em geolocalização para evitar acessos indesejados de localidades específicas.

Maior Controle da Solução: Aumento do controle sobre a solução adotada.

Manutenção Pós-Contrato: Garantia de que a solução continuará a proteger o ambiente corporativo, mesmo após o término do contrato, oferecendo pelo menos um nível básico de proteção.

Ademais, destaca-se que a presente contratação está devidamente alinhada às demandas e necessidades de negócio do Ministério, os benefícios a serem alcançados são adequados, os custos previstos são compatíveis e caracterizam a economicidade, e os riscos envolvidos são administráveis.

18. Providências a serem Adotadas

Para adequar o ambiente à instalação dos equipamentos e serviços da solução avançada de proteção de perímetro, garantindo um impacto mínimo na experiência dos usuários e beneficiários dos sistemas do Ministério das Cidades, as seguintes providências devem ser adotadas:

Nomear a equipe de execução: Designar claramente os colaboradores responsáveis pela implementação dos serviços e garantir que todos estejam cientes de suas funções e responsabilidades.

Elaborar um plano de execução detalhado: Criar um cronograma abrangente que inclua janelas de execução com prazos definidos e etapas bem delineadas, permitindo um gerenciamento eficaz do tempo e recursos.

Acompanhar e documentar as execuções: Estabelecer um processo de monitoramento contínuo durante a implementação, com a criação de relatórios detalhados após a conclusão de cada etapa, que incluam resultados, dificuldades encontradas e soluções aplicadas.

Definir prazos e horários de execução: Estipular prazos e horários para a realização dos serviços, garantindo a máxima transparência aos usuários e colaboradores. Isso inclui a comunicação prévia de eventuais interrupções nos serviços e os impactos esperados.

Fiscalizar a implementação dos serviços: Realizar uma supervisão rigorosa sobre a execução dos serviços implantados, assegurando que todas as definições e especificações técnicas estejam sendo cumpridas de acordo com o plano.

Promover treinamentos e orientações: Proporcionar sessões de treinamento para os usuários e colaboradores sobre a nova solução avançada de proteção de perímetro, explicando as mudanças, os benefícios e as práticas recomendadas de segurança.

Implementar um canal de comunicação: Criar um canal dedicado para que os usuários possam relatar problemas, dúvidas ou sugestões durante e após a implementação, assegurando que as preocupações sejam tratadas de forma ágil e eficiente.

Realizar testes pós-implementação: Após a instalação, conduzir testes abrangentes para garantir que a solução de proteção de perímetro esteja funcionando corretamente e que não haja impacto negativo nas operações dos sistemas do Ministério das Cidades.

Essas medidas são essenciais para garantir uma transição suave e eficiente para a nova solução avançada de proteção de perímetro, minimizando a interrupção das atividades diárias e promovendo a segurança da informação.

19. Declaração de Viabilidade

Esta equipe de planejamento declara **viável** esta contratação.

19.1. Justificativa da Viabilidade

Sendo evidente os benefícios identificados durante a etapa de estudo desta contratação, em termos de eficácia, eficiência, efetividade e economicidade. A solução escolhida trará diversos ganhos técnicos que serão registrados e avaliados ao longo do período de contratação.

Considerando as informações do presente estudo, entende-se que a presente contratação se configura econômica e tecnicamente **VIÁVEL**.

20. Responsáveis

Todas as assinaturas eletrônicas seguem o horário oficial de Brasília e fundamentam-se no §3º do Art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

EMERSON MOREIRA DE MORAIS

Integrante Requisitante

Assinou eletronicamente em 06/01/2025 às 14:56:18.

ALINE BARROS DE SOUSA

Integrante Técnico

Assinou eletronicamente em 06/01/2025 às 12:15:38.

LUCAS MENDES DOS SANTOS

AUTORIDADE MÁXIMA DA ÁREA DE TI

Assinou eletronicamente em 07/01/2025 às 11:20:29.